JP2000307588A

OPTICAL SUBSCRIBER LINE TERMINATING DEVICE AND OPTICAL SUBSCRIBER END STATION DEVICE

Publication number : JP2000307588A

Date of publication of application : 02.11.2000

Application number : 11-109687

Date of filing : 16.04.1999

Applicant : FUJITSU LTD

Inventor : KADOSAWA TAKASHI
MIURA KENJI
MATSUO TAMOTSU
SHIONO HIDEKI
TOYODA YOSHIMI
KOYANAGI TOSHINORI
ABIRU SETSUO
YASUSATO ATSUSHI
FUJIYOSHI SHINICHI
UCHIDA KAZUHIRO
RYU KAZUYA
HIRASHIMA KATSUHIKO
YOTSUMARU TAKEO
WAKAYOSHI MITSUHARU
SAKAI TOSHIYUKI

Abstract:
PROBLEM TO BE SOLVED: To efficiently execute the receiving control and decoding processing of information.

SOLUTION: A first storing means M11a stores ciphering setting information which is being used presently. A second storing means M11b stores newly updated ciphering setting information. A ciphering setting information storing means 11 includes the means M11a and the means M11b, executes storage control on the means M11a and the means M11b. A ciphered information deciphering processing means 12 receives an information stream having a frame constitution and then validates stored ciphering setting information from the next frame to execute deciphering processing to a ciphered information part shown by ciphering setting information from the next frame.

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号
特開2000－307588
（P2000－307588A）
(43)公開日　平成12年11月２日(2000.11.2)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード（参考）
Ｈ０４Ｌ　12/28		Ｈ０４Ｌ　11/20	Ｄ	５Ｊ１０４
Ｈ０４Ｂ　10/00		Ｈ０４Ｂ　9/00	Ｂ	５Ｋ００２
Ｈ０４Ｌ　9/08		Ｈ０４Ｌ　9/00	６０１Ｂ	５Ｋ０３０
9/16			６４３	５Ｋ０３３
12/44		11/00	３４０	５Ｋ０６９

審査請求　未請求　請求項の数29　ＯＬ　（全 44 頁）　最終頁に続く

(21)出願番号　特願平11－109687

(22)出願日　平成11年４月16日(1999.4.16)

(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号

(72)発明者　門澤　敬
大阪府大阪市中央区城見２丁目２番６号
富士通関西ディジタル・テクノロジ株式会社内

(74)代理人　100092152
弁理士　服部　毅巖

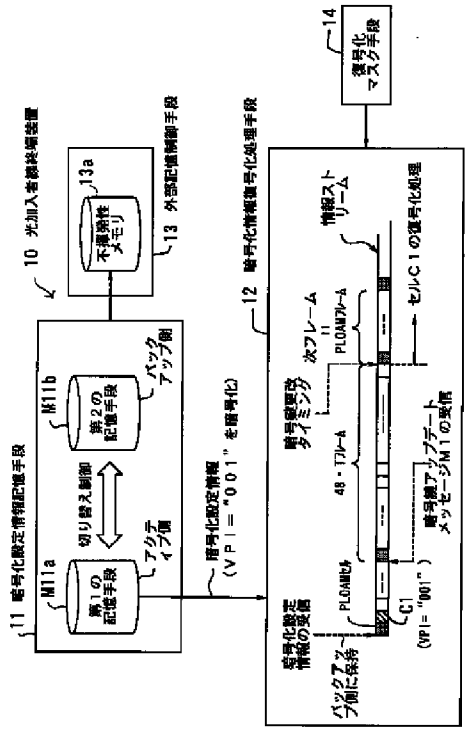
最終頁に続く

(54)【発明の名称】　光加入者線終端装置及び光加入者線端局装置

(57)【要約】

【課題】　情報の受信制御及び復号化処理を効率よく行う。

【解決手段】　第１の記憶手段Ｍ１１ａは、現在使用中の暗号化設定情報を記憶する。第２の記憶手段Ｍ１１ｂは、新しく更改された暗号化設定情報を記憶する。暗号化設定情報記憶手段１１は、第１の記憶手段Ｍ１１ａと第２の記憶手段Ｍ１１ｂを含み、第１の記憶手段Ｍ１１ａ及び第２の記憶手段Ｍ１１ｂへの記憶制御を行い、暗号鍵の暗号鍵更改タイミングで、第１の記憶手段Ｍ１１ａと第２の記憶手段Ｍ１１ｂとの切り替え制御を行う。暗号化情報復号化処理手段１２は、フレーム構成を持つ情報ストリームを受信した後、記憶している暗号化設定情報を次フレームから有効にして、暗号化設定情報が示す暗号化された情報部分に対する復号化処理を次フレームから行う。



【特許請求の範囲】
【請求項１】　光加入者系システムに接続して情報ストリームを受信し、暗号鍵を用いて、暗号化された情報部分の復号化を行う光加入者線終端装置において、
論理コネクション毎に暗号化を施したか否かを示す設定情報である暗号化設定情報に対し、現在使用中の暗号化設定情報を記憶するアクティブ側の第１の記憶手段と、新しく更改された暗号化設定情報を記憶するバックアップ側の第２の記憶手段とを含み、前記第１の記憶手段及び前記第２の記憶手段への記憶制御を行い、前記暗号鍵の暗号鍵更改タイミングで、前記第１の記憶手段と前記第２の記憶手段との切り替え制御を行う暗号化設定情報記憶手段と、
フレーム構成を持つ前記情報ストリームを受信し、記憶している前記暗号化設定情報を、前記暗号鍵更改タイミング以後の次フレームから有効にして、前記暗号化設定情報が示す暗号化された前記情報部分に対する復号化処理を前記次フレームから行う暗号化情報復号化処理手段と、
を有することを特徴とする光加入者線終端装置。
【請求項２】　前記暗号化設定情報記憶手段は、前記暗号鍵更改タイミングで前記第１の記憶手段と前記第２の記憶手段とを切り替えた後、あらたにアクティブ側になった第１の記憶手段に記憶してある前記暗号化設定情報を、あらたにバックアップ側になった第２の記憶手段へコピーすることを特徴とする請求項１記載の光加入者線終端装置。
【請求項３】　前記暗号化設定情報記憶手段は、バックアップ側の第２の記憶手段へのコピー中に、あらたな暗号化設定情報を受信した場合は、前記コピーの終了後に前記あらたな暗号化設定情報を前記第２の記憶手段に記憶することを特徴とする請求項２記載の光加入者線終端装置。
【請求項４】　前記暗号化設定情報記憶手段は、読み出しポートが２つある前記第１の記憶手段及び前記第２の記憶手段を含むことを特徴とする請求項１記載の光加入者線終端装置。
【請求項５】　前記暗号化設定情報記憶手段は、前記暗号化設定情報を受信して、前記第１の記憶手段または前記第２の記憶手段へ正常に書き込めた否かを検証し、正常に書き込めた場合にのみ応答信号を返送することを特徴とする請求項１記載の光加入者線終端装置。
【請求項６】　前記暗号化設定情報を不揮発性メモリに記憶させる外部記憶制御手段をさらに有することを特徴とする請求項１記載の光加入者線終端装置。
【請求項７】　前記外部記憶制御手段は、受信した前記暗号化設定情報と、バックアップ側の前記第２の記憶手段に格納されている暗号化設定情報とを比較し、異なる暗号化設定情報のみ前記不揮発性メモリに記憶させることを特徴とする請求項６記載の光加入者線終端装置。
【請求項８】　前記外部記憶制御手段は、前記暗号化設定情報をメモリに記憶させ、電源断時に前記メモリから前記不揮発性メモリへ、一括して前記暗号化設定情報を記憶させることを特徴とする請求項６記載の光加入者線終端装置。
【請求項９】　前記外部記憶制御手段は、前記暗号化設定情報をメモリに記憶させ、電源断時に前記メモリから前記不揮発性メモリへ、更改された暗号化設定情報のみ記憶させることを特徴とする請求項６記載の光加入者線終端装置。
【請求項１０】　前記暗号化設定情報記憶手段は、電源復旧時の立ち上げ準備状態の期間のみ、前記不揮発性メモリからの前記暗号化設定情報を受け付けることを特徴とする請求項６記載の光加入者線終端装置。
【請求項１１】　前記暗号化設定情報記憶手段は、電源復旧時に、前記不揮発性メモリから読み出された前記暗号化設定情報、またはあらたに送信された暗号化設定情報の一方を選択して有効にすることを特徴とする請求項６記載の光加入者線終端装置。
【請求項１２】　前記暗号化情報の復号化処理を行える運用状態から、他の状態へ遷移して、再度前記運用状態になった場合は、前記運用状態になった時から前記暗号鍵更改タイミングを受信するまでの期間の復号化処理をマスクする復号化マスク手段をさらに有することを特徴とする請求項１記載の光加入者線終端装置。
【請求項１３】　光加入者系システムに接続して情報ストリームを受信し、暗号鍵を用いて、暗号化された情報部分の復号化を行う光加入者線終端装置において、
論理コネクション毎に暗号化を施したか否かを示す設定情報である暗号化設定情報を記憶する暗号化設定情報記憶手段と、
フレーム構成を持つ前記情報ストリームを受信し、記憶している前記暗号化設定情報を次フレームから有効にして、前記暗号化設定情報が示す暗号化された前記情報部分に対する復号化処理を前記次フレームから行う暗号化情報復号化処理手段と、
を有することを特徴とする光加入者線終端装置。
【請求項１４】　光加入者系システムに接続して、暗号鍵を用いて暗号化を行った情報部分を含む情報ストリームを送信する光加入者線端局装置において、
受信装置へ前記情報ストリームを送信する際に、フラグの設定制御を行うフラグ設定制御手段と、
前記フラグにもとづいて、論理コネクション毎に暗号化を施したか否かを示す設定情報である暗号化設定情報の送信制御を行う暗号化設定情報送信制御手段と、
を有することを特徴とする光加入者線端局装置。
【請求項１５】　前記フラグ設定制御手段は、初期暗号化フラグを有し、前記初期暗号化フラグを前記受信装置が停止状態でクリア、初期暗号化の完了時にセットすることを特徴とする請求項１４記載の光加入者線端局装

置。

【請求項１６】　前記フラグ設定制御手段は、初期暗号化の実行中を示す初期暗号化実行中フラグを有することを特徴とする請求項１４記載の光加入者線端局装置。

【請求項１７】　前記フラグ設定制御手段は、前記受信装置に対する前記暗号化設定情報の設定更改が失敗と判断した場合は、設定更改失敗フラグをセットすることを特徴とする請求項１４記載の光加入者線端局装置。

【請求項１８】　前記フラグ設定制御手段は、前記受信装置が状態落ちしたと判断した場合は、設定更改未完了フラグをセットすることを特徴とする請求項１４記載の光加入者線端局装置。

【請求項１９】　前記フラグ設定制御手段は、暗号化の更改周期中に暗号化更改中フラグをセットすることを特徴とする請求項１４記載の光加入者線端局装置。

【請求項２０】　前記フラグ設定制御手段は、前記暗号化設定情報の設定更改を行う際には、設定更改要求フラグをセットすることを特徴とする請求項１４記載の光加入者線端局装置。

【請求項２１】　前記フラグ設定制御手段は、１つの前記受信装置につき、１つの前記論理コネクションの更改に対して、前記設定更改要求フラグをセットすることを特徴とする請求項２０記載の光加入者線端局装置。

【請求項２２】　前記フラグ設定制御手段は、前記暗号化設定情報の設定更改実行中には、設定更改実行中フラグをセットすることを特徴とする請求項１４記載の光加入者線端局装置。

【請求項２３】　前記暗号化設定情報を前記受信装置へ再度送信する上書き処理を行う暗号化設定情報上書き手段をさらに有することを特徴とする請求項１４記載の光加入者線端局装置。

【請求項２４】　前記暗号化設定情報上書き手段は、優先度の高い他のメッセージの送信を行う場合は、前記上書き処理を待機させることを特徴とする請求項２３記載の光加入者線端局装置。

【請求項２５】　前記暗号化設定情報上書き手段は、前記暗号化設定情報の設定更改実行中は、前記上書き処理を待機させることを特徴とする請求項２３記載の光加入者線端局装置。

【請求項２６】　前記暗号化設定情報上書き手段は、タイマを有し、前記タイマに設定された周期にしたがって、前記上書き処理を行うことを特徴とする請求項２３記載の光加入者線端局装置。

【請求項２７】　前記タイマの周期は、外部から任意の値に設定されることを特徴とする請求項２６記載の光加入者線端局装置。

【請求項２８】　前記暗号化設定情報送信制御手段は、前記暗号化設定情報を複数回送信する場合に、１回目の前記暗号化設定情報の送信時のみ他メッセージと調停処理を行い、調停後は前記暗号化設定情報を一定間隔毎に自動的に送信することを特徴とする請求項１４記載の光加入者線端局装置。

【請求項２９】　前記暗号鍵の暗号鍵更改タイミングで、前記暗号化設定情報の更改を開始する暗号化設定情報更改手段をさらに有することを特徴とする請求項１４記載の光加入者線端局装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は光加入者線終端装置及び光加入者線端局装置に関し、特に光加入者系システムに接続して情報ストリームを受信し、暗号鍵を用いて、暗号化された情報部分の復号化を行う光加入者線終端装置、及び光加入者系システムに接続して、暗号鍵を用いて暗号化を行った情報部分を含む情報ストリームを送信する光加入者線端局装置に関する。

【０００２】

【従来の技術】近年、通信サービスの多様化は加速し、ビデオ・オン・デマンド、ＣＡＴＶ、高速コンンピュータ通信等の需要が拡大しつつある。このような大容量の通信サービスを低料金で提供するためには、加入者通信網を光化した光加入者系システムが不可欠である。

【０００３】光加入者系システムとしては、１本の光ファイバを複数の加入者で共有するＰＤＳ（Passive Double Star)が提案されている。また、特に欧州を中心にしてＰＤＳ方式を採用したＰＯＮ（Passive Optical Network)システムが注目されており、光ファイバを各家庭まで敷設するＦＴＴＨ（Fiber To The Home)システムの実現へ向けて開発が進んでいる。

【０００４】また、このようなＦＴＴＨシステムの実現のためには、音声や動画などのリアルタイムの通信要求に対して、通信帯域や品質を保証するために、ＡＴＭ（Asynchronous Transfer Mode）を利用したＡＴＭ－ＰＯＮの構築が、ＦＳＡＮ（FullService Access Networks：光通信事業を推進するために設立された国際的な通信業界団体）を中心に進められている。

【０００５】図２５はＡＴＭ－ＰＯＮシステムの構成を示す図である。加入者宅１００ａ～１００ｎ内には、光バースト伝送を行うＯＮＵ（Optical Network Unit：光加入者線終端装置）１０１ａ～１０１ｎが配置され、局２００内にはＯＬＴ（Optical Line Terminal ：光加入者線端局装置）２０１が配置される。

【０００６】ＯＮＵ１０１ａ～１０１ｎには電話機やＣＡＴＶ等が接続され、ＯＬＴ２０１には交換機（ＡＴＭ交換機、ＩＳＤＮ交換機等）２０２が接続する。また、ＯＮＵ１０１ａ～１０１ｎとＯＬＴ２０１は、スターカプラ３００と接続する。

【０００７】局２００から加入者宅１００ａ～１００ｎへの下り情報（下りセル）は、１本の光ファイバから、スターカプラ３００を介して、樹枝状に分岐された光ファイバを通じて送信される。また、加入者宅１００ａ～

１００ｎから局２００への上り情報（上りセル）は、樹枝状に分岐された光ファイバから、スターカプラ３００を介して、１本に集約された光ファイバを通じて送信される。

【０００８】このように、ＡＴＭ－ＰＯＮシステムは、スターカプラ３００で局と複数の加入者とを１：ｎで接続して構成する、ＡＴＭを使った光分岐型のアクセスネットワークである。

【０００９】ここで、ＯＬＴ２０１からＯＮＵ１０１ａ～１０１ｎへの下り通信は、放送型であるため、ＩＴＵ－Ｔ勧告Ｇ．９８３では、ＯＮＵ毎の秘匿性を目的として、暗号化（Ｃｈｕｒｎｉｎｇ）方式が規定されている。

【００１０】まず、ＯＬＴ２０１は、下りメッセージにより、ＯＮＵ（例えば、ＯＮＵ１０１ａ）に暗号鍵を要求する。すると、応答したＯＮＵ１０１ａは、暗号鍵を生成し、ＯＬＴ２０１に通知する。

【００１１】ＯＬＴ２０１は、その暗号鍵を使用して、ＯＮＵ１０１ａに対して送信すべき下り情報に対して暗号化を施す。この下り情報の暗号化はＶＰ（Virtual Path：仮想パス）毎に行われる。

【００１２】この場合、ＯＬＴ２０１は、ＯＮＵ１０１ａに対し、ＶＰＩ（Virtual Path Identifier ：仮想パス識別子）を単位として、どのＶＰに対して暗号化を施した（ＯＮ）か否か（ＯＦＦ）を示す設定情報である暗号化設定情報を下りメッセージにより通知する。

【００１３】このように、ＡＴＭ－ＰＯＮシステムの暗号化方式では、暗号鍵はＯＮＵ毎に割り当てられ、下り情報の暗号化のＯＮ／ＯＦＦはＶＰＩ単位で行われる。そして、ＯＬＴ２０１がＯＮＵ１０１ａに下りメッセージを用いて、暗号化設定情報を通知し、ＯＮＵ１０１ａでは自己の暗号鍵を用いて、暗号化されたＶＰの下り情報を復号化する。

【００１４】

【発明が解決しようとする課題】しかし、上記のようなＩＴＵ－Ｔ勧告Ｇ．９８３におけるＡＴＭ－ＰＯＮシステムの暗号化方式では、詳細な処理手順が規定されていない。

【００１５】例えば、ＯＮＵ１０１ａでは、ＯＬＴ２０１からの暗号化設定情報を保持しているが、ＩＴＵ－Ｔ勧告Ｇ．９８３には復号化処理をいつ有効にすべきかが規定されていない。

【００１６】したがって、ＯＬＴ２０１側での暗号化処理、ＯＮＵ１０１ａ側での復号化処理それぞれに時間的に大きなずれがあった場合などでは、暗号化・復号化が正常に行えないといった問題があった。

【００１７】また、暗号化設定情報は、ＯＮＵの電源断時にはリセットされるため、電源復旧後は再度設定を行う必要があり、再立ち上げに時間がかかるなどといった問題もある。

【００１８】このように、従来のＡＴＭ－ＰＯＮシステムの暗号化方式では、十分な技術が未だ確立されておらず、システム構築の実現のために高品質な通信制御を早急に確立する必要がある。

【００１９】本発明はこのような点に鑑みてなされたものであり、高品質な通信制御を確立し、情報の受信制御及び復号化処理を効率よく行う光加入者線終端装置を提供することを目的とする。

【００２０】また、本発明の他の目的は、高品質な通信制御を確立し、情報の送信制御を効率よく行う光加入者線端局装置を提供することである。

【００２１】

【課題を解決するための手段】本発明では上記課題を解決するために、図１に示すような、光加入者系システムに接続して情報ストリームを受信し、暗号鍵を用いて、暗号化された情報部分の復号化を行う光加入者線終端装置１０において、論理コネクション毎に暗号化を施したか否かを示す設定情報である暗号化設定情報に対し、現在使用中の暗号化設定情報を記憶するアクティブ側の第１の記憶手段Ｍ１１ａと、新しく更改された暗号化設定情報を記憶するバックアップ側の第２の記憶手段Ｍ１１ｂとを含み、第１の記憶手段Ｍ１１ａ及び第２の記憶手段Ｍ１１ｂへの記憶制御を行い、暗号鍵の暗号鍵更改タイミングで、第１の記憶手段Ｍ１１ａと第２の記憶手段Ｍ１１ｂとの切り替え制御を行う暗号化設定情報記憶手段１１と、フレーム構成を持つ情報ストリームを受信し、記憶している暗号化設定情報を、暗号鍵更改タイミング以後の次フレームから有効にして、暗号化設定情報が示す暗号化された情報部分に対する復号化処理を次フレームから行う暗号化情報復号化処理手段１２と、を有することを特徴とする光加入者線終端装置１０が提供される。

【００２２】ここで、第１の記憶手段Ｍ１１ａは、現在使用中の暗号化設定情報を記憶する。第２の記憶手段Ｍ１１ｂは、新しく更改された暗号化設定情報を記憶する。暗号化設定情報記憶手段１１は、第１の記憶手段Ｍ１１ａと第２の記憶手段Ｍ１１ｂを含み、第１の記憶手段Ｍ１１ａ及び第２の記憶手段Ｍ１１ｂへの記憶制御を行い、暗号鍵の暗号鍵更改タイミングで、第１の記憶手段Ｍ１１ａと第２の記憶手段Ｍ１１ｂとの切り替え制御を行う。暗号化情報復号化処理手段１２は、フレーム構成を持つ情報ストリームを受信し、記憶している暗号化設定情報を、暗号鍵更改タイミング以後の次フレームから有効にして、暗号化設定情報が示す暗号化された情報部分に対する復号化処理を次フレームから行う。

【００２３】また、図１５に示すような、光加入者系システムに接続して、暗号鍵を用いて暗号化を行った情報部分を含む情報ストリームを送信する光加入者線端局装置２０において、受信装置へ情報ストリームを送信する際に、フラグの設定制御を行うフラグ設定制御手段２１

と、フラグにもとづいて、論理コネクション毎に暗号化を施したか否かを示す設定情報である暗号化設定情報の送信制御を行う暗号化設定情報送信制御手段２２と、を有することを特徴とする光加入者線端局装置２０が提供される。

【００２４】ここで、フラグ設定制御手段２１は、受信装置へ情報ストリームを送信する際に、フラグの設定制御を行う。暗号化設定情報送信制御手段２２は、フラグにもとづいて、論理コネクション毎に暗号化を施したか否かを示す設定情報である暗号化設定情報の送信制御を行う。

【００２５】

【発明の実施の形態】以下、本発明の実施の形態を図面を参照して説明する。図１は本発明の光加入者線終端装置の原理図である。光加入者線終端装置１０は、ＯＮＵに該当し、ＡＴＭ－ＰＯＮ等の光加入者系システムに接続してＯＬＴから送信される情報ストリーム（複数のセルで構成される）を受信する。

【００２６】そして、自己の装置で生成した暗号鍵を用いて、情報ストリーム内の暗号化された情報部分に対して復号化を行う。以降では、光加入者線終端装置１０をＯＮＵ１０と呼ぶ。

【００２７】暗号化設定情報記憶手段１１は、暗号化設定情報を記憶するために、第１の記憶手段Ｍ１１ａと第２の記憶手段Ｍ１１ｂの２面の記憶領域を有している。ここで、暗号化設定情報とは、論理コネクション毎に暗号化を施したか否かを示す設定情報である。具体的には、ＶＰＩを単位として、どのＶＰに対して暗号化を施したか否かを示す設定情報のことをいう。

【００２８】第１の記憶手段Ｍ１１ａは、アクティブ側であり、現在使用中（読み出し中）の暗号化設定情報を記憶している。第２の記憶手段Ｍ１１ｂは、バックアップ側であり、新しく更改された暗号化設定情報を記憶する。

【００２９】そして、暗号化設定情報記憶手段１１は、第１の記憶手段Ｍ１１ａと第２の記憶手段Ｍ１１ｂへの記憶制御（書き込み制御）を行い、暗号鍵の暗号鍵更改タイミング（古い暗号鍵を新しい暗号鍵に更改した時のタイミング）で、第１の記憶手段Ｍ１１ａと第２の記憶手段Ｍ１１ｂとの切り替え制御を行う。詳細は後述する。

【００３０】暗号化情報復号化処理手段１２は、フレーム構成を持つ情報ストリームを受信し、記憶している暗号化設定情報を第１の記憶手段Ｍ１１ａから読み出して、暗号鍵更改タイミング以後の次フレームから、読み出した暗号化設定情報を有効にする。そして、暗号化設定情報が示す暗号化された情報部分に対する復号化処理を次フレームから行う。

【００３１】例えば、情報ストリーム中の１つのフレームの中で、ＶＰＩ＝“００１”（“００１”はヘキサデータ）の情報が暗号化されている旨が暗号化設定情報に記載されているものとする。また、ＶＰＩ＝“００１”に対応するセルがセルＣ１だとする。

【００３２】図に示すように、暗号化設定情報を受信すると、バックアップ側の第２の記憶手段Ｍ１１ｂに記憶する。その後、暗号鍵アップデートメッセージＭ１を受信して、４８×Ｔフレーム経過した後の暗号鍵更改タイミング以後の次フレームからこの暗号化設定情報を有効にする。このようにして復号化処理の有効タイミングを明確に規定したので、暗号化処理、復号化処理の不一致を防止することが可能になる。なお、詳細動作は後述する。

【００３３】外部記憶制御手段１３は、暗号化設定情報を不揮発性メモリ１３ａに記憶させる。復号化マスク手段１４は、暗号化情報の復号化を行える運用状態から、他の状態へ遷移して再度運用状態になった場合に、運用状態になった時から暗号鍵更改タイミングを受信するまでの期間の復号化処理をマスクする。なお、外部記憶制御手段１３及び復号化マスク手段１４の詳細については後述する。

【００３４】次に本発明のＯＮＵ１０の具体的な構成・動作について詳しく説明する。なお、以降では暗号化処理をＣｈｕｒｎ、復号化処理をＤｅｃｈｕｒｎ、暗号化設定情報をＣｈｕｒｎｅｄ－ＶＰ設定情報と呼ぶ。

【００３５】図２は情報ストリームの構成及びＣｈｕｒｎｅｄ－ＶＰ設定情報のフォーマットを示す図である。ＯＬＴから送信される情報ストリームの１つのフレーム（ＰＬＯＡＭフレーム）は、ＯＬＴとＯＮＵ１０間で制御情報を通信するためのＰＬＯＡＭ（Physical Layer Operation And Management ）セルと、実際の通信情報であるユーザセルＣ１～Ｃ２７から構成される。そして、このＰＬＯＡＭフレーム２つ分で、Ｔフレームと呼ぶ（伝送レートが１５０Ｍｂｐｓモードの場合）。また、ＰＬＯＡＭセル及びユーザセル共に、１セルが５３バイトである。

【００３６】Ｃｈｕｒｎｅｄ－ＶＰ設定情報は、ＰＬＯＡＭセルで送信される各種制御情報のうちの１つであり、ＰＬＯＡＭセルの４０バイト～５１バイトまでがＣｈｕｒｎｅｄ－ＶＰ設定情報として定義されている。

【００３７】４０バイト目は、ＰＯＮ－ＩＤであり、ＯＮＵ１０の識別子としてＰＯＮ－ＩＤが記される。４１バイト目は、Ｃｈｕｒｎｅｄ－ＶＰ設定情報であることを知らせる識別子が記される。この識別子は“００００１１１１”（左側がＭＳＢ、右側がＬＳＢである。以降同様）である。

【００３８】４３、４４バイト目は、ＶＰＩを示す情報であり、４３、４４バイト目に記されるＶＰＩ情報をＶＰＩ〔１１：０〕と表す。また、４３バイト目の“ａｂｃｄｅｆｇｈ”をＶＰＩ〔１１：４〕と表し、４４バイト目の“ｉｊｋｌ”をＶＰＩ〔３：０〕と表す。なお、

ＡＴＭ－ＰＯＮシステムのＶＰＩの値は４０９６個ある（４０９６ＶＰある）。また、ユーザセルも、どのＶＰから流れてきたものかを示すために、同様なＶＰＩ情報をそれぞれ個別に有している。

【００３９】ここで、〔Ｍ：Ｎ〕は、下位Ｎビットから上位Ｍビットの（Ｍ－Ｎ＋１）ビットのデータであることを意味する。４２バイト目は、４３、４４バイト目に記されたＶＰＩに対して、Ｃｈｕｒｎされているか否かを示す情報が記される。内容は“ｘｘｘｘｘｘｘａ”（ｘ＝未定義）であり、ａ（アクトビット）＝１ならＣｈｕｒｎされており（したがって、ＯＮＵ１０ではＤｅｃｈｕｒｎしなければならない）、ａ＝０ならＣｈｕｒｎされていない。４５～５１バイト目は未定である。

【００４０】図３は次フレームでＤｅｃｈｕｒｎを実現するためのブロック構成を示す図である。なお、Ｃｈｕｒｎｅｄ－ＶＰメッセージフラグ設定手段１１－１とＣｈｕｒｎｅｄ－ＶＰ設定情報書き込み手段１１－２は暗号化設定情報記憶手段１１内に含まれ、復号化処理手段１２は暗号化情報復号化処理手段１２に対応する。

【００４１】Ｃｈｕｒｎｅｄ－ＶＰメッセージフラグ設定手段１１－１は、ＰＬＯＡＭセルのＣｈｕｒｎｅｄ－ＶＰ設定情報を受信した場合に、Ｃｈｕｒｎｅｄ－ＶＰメッセージフラグをセットする。

【００４２】Ｃｈｕｒｎｅｄ－ＶＰ設定情報書き込み手段１１－２は、Ｃｈｕｒｎｅｄ－ＶＰメッセージフラグをライトイネーブルの１つとして用い、ＲＡＭ１１ａ（暗号化設定情報記憶手段１１が含む記憶手段に対応する）にＣｈｕｒｎｅｄ－ＶＰ設定情報の書き込みを行う。ＲＡＭ１１ａは、２５６アドレスであり、１アドレスが格納するデータ領域は１６ビットある。

【００４３】書き込み処理としては、ＶＰＩ〔１１：０〕のうち、ＶＰＩ〔１１：４〕の８ビットをＲＡＭ１１ａへの書き込みアドレスとし、ａビット情報をＲＡＭ１１ａへの書き込みデータとする。

【００４４】ここで、ＶＰＩ〔１１：４〕をＲＡＭ１１ａのアドレスとした場合に、この１つのアドレスに１６ビットの格納領域があるため、１アドレスにＶＰＩ〔３：０〕（４ビット）の１６通りのＶＰＩ値を割り当てることができる。

【００４５】すなわち、ＲＡＭの１つのアドレスに対して、１６通りのＶＰＩを設定でき、この１６通りのＶＰＩに対応するａビット情報を、ＲＡＭ１１ａの格納領域である１６ビットの各ビットに対してデータとして書き込んでいく。したがって、ＲＡＭ１１ａは、４０９６個のａビット情報の記憶領域を有することになる。

【００４６】復号化処理手段１２は、情報ストリームを受信し、ユーザセルに記載されているＶＰＩ〔１１：０〕を抽出する。そして、抽出したＶＰＩ〔１１：０〕のＶＰＩ〔１１：４〕をＲＡＭ１１ａへの読み出しアドレスとし、ＶＰＩ〔３：０〕に対応する位置にあるビットのａビット情報を読み出しデータとする。ａビット情報＝１ならば、そのセルを暗号鍵を用いてＤｅｃｈｕｒｎし、ａビット情報＝０ならば、ＮｏｔＤｅｃｈｕｒｎ（復号化を行わずスルー）とする。

【００４７】図４は次フレームからＤｅｃｈｕｒｎを行う際のタイミングチャートを示す図である。情報ストリームのＰＬＯＡＭセルａのＣｈｕｒｎｅｄ－ＶＰ設定情報に、ＶＰＩ〔１１：０〕＝“００１”（“００１”はヘキサデータ）の情報がＣｈｕｒｎされている（ａビット情報＝１）旨が記載されているものとする。

【００４８】Ｃｈｕｒｎｅｄ－ＶＰメッセージフラグ設定手段１１－１は、ＰＬＯＡＭセルａを受信して、４１バイト目のＣｈｕｒｎｅｄ－ＶＰ設定情報のＩＤを認識すると、Ｃｈｕｒｎｅｄ－ＶＰメッセージフラグを図に示す位相で出力する。

【００４９】また、Ｃｈｕｒｎｅｄ－ＶＰ設定情報書き込み手段１１－２は、ＶＰＩ〔１１：０〕＝“００１”及びａビット情報（＝１）を次フレームのユーザセルＣ１の区間まで内部でラッチする。

【００５０】そして、Ｃｈｕｒｎｅｄ－ＶＰメッセージフラグとＰＬＯＡＭパルス（ＰＬＯＡＭセルの位置を示すパルス）との論理をとった信号をライトイネーブルとして、図に示すセルＦＰ（セルの位置を示すパルス）の位置で、ＶＰＩ〔１１：４〕＝“００”をＲＡＭ１１ａの書き込みアドレス、１６ビットのＶＰＩ〔３：０〕＝“１”の位置にａビット情報を書き込みデータとしてＲＡＭ１１ａに書き込む。

【００５１】このように、ＰＬＯＡＭセルａを受信した後、次フレームのＰＬＯＡＭセルｂの先頭位置でＰＬＯＡＭセルａにあったＣｈｕｒｎｅｄ－ＶＰ設定情報をＲＡＭ１１ａに書き込み、その後、復号化処理手段１２で読み出して、図に示す位置Ａ（次フレームのユーザセルＣ１の先頭）からＶＰＩ〔１１：０〕＝“００１”に対応するセルのＤｅｃｈｕｒｎを行っていく。ここではＶＰＩ〔１１：０〕＝“００１”はセルＣ１としたので、位置Ａからセル Ｃ１のＤｅｃｈｕｒｎが行われる。

【００５２】一方、情報ストリームのＰＬＯＡＭセルｂのＣｈｕｒｎｅｄ－ＶＰ設定情報に、ＶＰＩ〔１１：０〕＝“０１０”とあり、Ｃｈｕｒｎされていない（ａビット情報＝０）旨が記載されている場合には、図に示すようなタイミングでＶＰＩ〔１１：０〕＝“０１０”はＮｏｔＤｅｃｈｕｒｎとなる。

【００５３】このように、本発明のＯＮＵ１０では、ＯＬＴがＰＬＯＡＭセルに設定したＣｈｕｒｎｅｄ－ＶＰ設定情報を、次フレームにあるＰＬＯＡＭセル以降から有効にするような構成とした。

【００５４】これにより、次フレームのユーザセルから即時にＤｅｃｈｕｒｎ処理を行うことができるので、暗号化処理と復号化処理の不一致防止、さらにデータ疎通時間を短縮させることが可能になる。

【００５５】次に暗号鍵更改について説明する。本発明のＯＮＵ１０が適用されるＡＴＭ－ＰＯＮシステムでは、ＯＬＴ側に位置する保守端末装置からの要求毎に、暗号鍵（以降、Ｃｈｕｒｎｉｎｇ－Ｋｅｙと呼ぶ）の更改（鍵を新しくすること）を行っている。図５はＣｈｕｒｎｉｎｇ－Ｋｅｙの更改シーケンスを示す図である。

〔Ｓ１〕ＯＬＴは、新しいＣｈｕｒｎｉｎｇ－Ｋｅｙの送信要求として、Ｃｈｕｒｎｉｎｇ－Ｋｅｙアップデートメッセージｍ１をＯＮＵ１０に送信する。

〔Ｓ２〕ＯＮＵ１０は、新しいＣｈｕｒｎｉｎｇ－Ｋｅｙを生成して、ＡＣＫメッセージｍ１に乗せてＯＬＴに返送する。

〔Ｓ３〕ＯＬＴは、Ｃｈｕｒｎｉｎｇ－Ｋｅｙアップデートメッセージｍ１を送信してから１６×Ｔフレーム経過した後、Ｃｈｕｒｎｉｎｇ－Ｋｅｙアップデートメッセージｍ２をＯＮＵ１０に送信する。

〔Ｓ４〕ＯＮＵ１０は、ステップＳ２と同様に、ＡＣＫメッセージｍ２に更改したＣｈｕｒｎｉｎｇ－Ｋｅｙの情報を乗せてＯＬＴに返送する。

〔Ｓ５〕ＯＬＴは、Ｃｈｕｒｎｉｎｇ－Ｋｅｙアップデートメッセージｍ２を送信してから１６×Ｔフレーム経過した後、Ｃｈｕｒｎｉｎｇ－Ｋｅｙアップデートメッセージｍ３をＯＮＵ１０に送信する。

〔Ｓ６〕ＯＮＵ１０は、ステップＳ２及びステップＳ４と同様に、ＡＣＫメッセージｍ３をＯＬＴに返送する。

〔Ｓ７〕ＯＬＴがＣｈｕｒｎｉｎｇ－Ｋｅｙアップデートメッセージｍ１をＯＮＵ１０へ送信してから４８×Ｔフレーム経過した時点（Ｃｈｕｒｎｉｎｇ－Ｋｅｙ更改タイミング）で、新しいＣｈｕｒｎｉｎｇ－Ｋｅｙが使用される。すなわち、ＯＬＴはこの新しいＣｈｕｒｎｉｎｇ－ＫｅｙでＣｈｕｒｎを行い、ＯＮＵ１０は新しいＣｈｕｒｎｉｎｇ－ＫｅｙでＤｅｃｈｕｒｎを行う。なお、１６×Ｔフレームのカウントは、図に示すようにＯＬＴ、ＯＮＵ１０の双方で行う。

【００５６】したがって、ＯＬＴがＣｈｕｒｎｉｎｇ－Ｋｅｙアップデートメッセージｍ１をＯＮＵ１０に送信してから、４８×Ｔフレーム経過するまでは、旧タイプのＣｈｕｒｎｉｎｇ－Ｋｅｙを用いて、ＯＬＴとＯＮＵ１０間でＣｈｕｒｎ／Ｄｅｃｈｕｒｎが行われる。

【００５７】次に暗号化設定情報記憶手段１１の２面ＲＡＭ構成及びコピー動作について説明する。図５で説明したように、Ｃｈｕｒｎｉｎｇ－ＫｅｙをＣｈｕｒｎｉｎｇ－Ｋｅｙ更改タイミングで更改した場合には、Ｃｈｕｒｎｅｄ－ＶＰ設定情報もこのタイミングでＯＮＵ１０側で更改しなければならない。したがって、Ｃｈｕｒｎｉｎｇ－Ｋｅｙ更改タイミングとなる以前にＯＬＴから送信された新しいＣｈｕｒｎｅｄ－ＶＰ設定情報を記憶しておく必要がある。

【００５８】図６は２面ＲＡＭを持つＯＮＵ１０のブロック構成を示す図である。図３で説明した構成に対して、あらたにＲＡＭ１１ｂと、切り替え制御手段１１－３、コピー制御手段１１－４が付加されている。切り替え制御手段１１－３とコピー制御手段１１－４は暗号化設定情報記憶手段１１内に含まれる。

【００５９】最初、ＲＡＭ１１ａを、アクティブ側（ＶＰＩ〔１１：４〕をアドレスとして現在Ｃｈｕｒｎｅｄ－ＶＰ設定情報が読み出されているＲＡＭ）とし、ＲＡＭ１１ｂをバックアップ側（ＯＬＴから送信された新しいＣｈｕｒｎｅｄ－ＶＰ設定情報を次のＣｈｕｒｎｉｎｇ－Ｋｅｙ更改タイミングまで保持しておくＲＡＭ）とする。

【００６０】切り替え制御手段１１－３は、Ｃｈｕｒｎｉｎｇ－ＫｅｙアップデートメッセージＭ１～Ｍ３を３回受信して、Ｃｈｕｒｎｉｎｇ－ＫｅｙアップデートメッセージＭ１から４８×Ｔフレーム経過した場合には、その時間をＣｈｕｒｎｉｎｇ－Ｋｅｙ更改タイミングとして認識する。

【００６１】そして、Ｃｈｕｒｎｉｎｇ－Ｋｅｙ更改タイミングでＲＡＭ１１ａとＲＡＭ１１ｂを切り替えて、ＲＡＭ１１ｂをアクティブ側、ＲＡＭ１１ａをバックアップ側とする。

【００６２】一方、このままでは古いＣｈｕｒｎｅｄ－ＶＰ設定情報を記憶しているＲＡＭ１１ａがバックアップ側となってしまう。したがって、コピー制御手段１１－４は、新しくアクティブ側になったＲＡＭ１１ｂからデータをＲＡＭ１１ａへコピーしていく。

【００６３】なお、ＲＡＭ１１ａ及びＲＡＭ１１ｂは共に読み出しポートを２つ有している。このため、例えば、アクティブ側のＲＡＭからバックアップ側のＲＡＭへコピーが行われている最中でも、アクティブ側ＲＡＭからＣｈｕｒｎｅｄ－ＶＰ設定情報を読み出すことができる。

【００６４】図７はコピー動作手順を示すフローである。なお、最初はＲＡＭ１１ａをアクティブ側、ＲＡＭ１１ｂをバックアップ側とし、ＲＡＭ１１ａとＲＡＭ１１ｂのそれぞれは、図に示すような値（例えば、“０００”＝１とは、ＶＰＩ＝“０００”のａビット情報が１ということ）が格納されているものとする。

〔Ｓ１０〕切り替え制御手段１１－３は、Ｃｈｕｒｎｉｎｇ－Ｋｅｙ更改タイミングでＲＡＭ１１ａとＲＡＭ１１ｂを切り替える。

〔Ｓ１１〕コピー制御手段１１－４は、切り替え制御手段１１－３から通知されたＣｈｕｒｎｉｎｇ－Ｋｅｙ更改タイミングを受信すると、ＲＡＭ１１ｂに対する読み出しアドレスをインクリメントして、ＲＡＭ１１ｂからデータを読み出す。

〔Ｓ１２〕コピー制御手段１１－４は、ＲＡＭ１１ａに対する書き込みアドレスをインクリメントして、ＲＡＭ１１ｂから読み出したデータをＲＡＭ１１ａへ書き込んでいく。

〔Ｓ１３〕コピー制御手段１１－４は、書き込みアドレスが最大になったか否かを判断する。最大でなければステップＳ１１へ戻って、ステップＳ１１、Ｓ１２を繰り返し行い、最大であればコピーを終了する。

【００６５】図８はコピー動作時のタイミングチャートを示す図である。ＫＥＹＴＩＭは、Ｃｈｕｒｎｉｎｇ－Ｋｅｙ更改タイミングパルスである。ＲＡＭ－ＳＴＡＴＥは、２面のＲＡＭがアクティブ側かバックアップ側かを示す信号であり、図では更改前のＲＡＭステートとしてＲＡＭ（Ｂ）がアクティブ側であり、更改後にＲＡＭ（Ａ）がアクティブ側となるものとする。

【００６６】ＣＯＰＹＭＯＤＥは、コピー動作時に“Ｈ”となる信号である。ＣＯＰＹＣＴＲは、ＣＯＰＹＭＯＤＥが“Ｈ”の間、ＲＡＭの２５６アドレス数をカウントするための信号である。実際には、ＸＷＥが図に示すような位相となるので、２５９進カウンタを用いている。

【００６７】ＲＡＭＡ－ＲＡＤは、新しくアクティブ側になったＲＡＭ（Ａ）の読み出しアドレスを示す信号であり、ＣＯＰＹＣＴＲを１段ずらした信号を読み出しアドレスとして使用する。

【００６８】ＲＡＭＡ－ＲＤＴは、ＲＡＭＡ－ＲＡＤのアドレスで読み出された読み出しデータを示す信号であり、アドレス０に対して読み出しデータＡ、アドレス１に対して読み出しデータＢ、……である。ＲＡＭＡ－ＲＡＤから１段ずれた位置に読み出しデータが出力される。

【００６９】ＲＡＭＢ－ＷＤＴは、バックアップ側となったＲＡＭ（Ｂ）への書き込みデータを示す信号であり、ＲＡＭＡ－ＲＤＴを１段ずらした信号を書き込みデータとして使用する。

【００７０】ＲＡＭＢ－ＷＡＤは、ＲＡＭＢ－ＷＤＴをＲＡＭ（Ｂ）へ書き込むための書き込みアドレスを示す信号である。アドレス０に対して書き込みデータＡ、アドレス１に対して書き込みデータＢ、……をＲＡＭ（Ｂ）へ書き込んでいく（コピーする）。

【００７１】ＸＷＥは、バックアップ側となったＲＡＭ（Ｂ）へ、ＲＡＭ（Ａ）の内容をコピーする場合の書き込みイネーブル信号であり、アクティブ“Ｌ”である。以上説明したように、本発明では、２面あるＲＡＭの切り替えを行った場合に、新しいＣｈｕｒｎｅｄ－ＶＰ設定情報を、切り替え後にバックアップ側となったＲＡＭへコピーする構成にした。

【００７２】これにより、バックアップ側も新しいＣｈｕｒｎｅｄ－ＶＰ設定情報を絶えず持つことができ、ＯＬＴ側とのＣｈｕｒｎｅｄ－ＶＰ設定情報の不一致を防止することが可能になる。

【００７３】次にコピー中にあらたなＣｈｕｒｎｅｄ－ＶＰ設定情報を受信した場合の動作について説明する。Ｃｈｕｒｎｉｎｇ－Ｋｅｙ更改タイミングは、ＰＬＯＡＭ周期を最小単位として、フレーム数を数えているので必ずＰＬＯＡＭセルの位置で上がることになる。

【００７４】この場合、Ｃｈｕｒｎｉｎｇ－Ｋｅｙ更改タイミングの位置のＰＬＯＡＭセルがＣｈｕｒｎｅｄ－ＶＰ設定情報を持つセルの場合、バックアップ側のＲＡＭへは、アクティブ側のＲＡＭのデータのコピーが開始されているため、その情報をバックアップ側のＲＡＭへ即時に書き込むことができない。

【００７５】そこで、コピー中にこのようなＣｈｕｒｎｅｄ－ＶＰ設定情報を受信した場合には、フラグ（上述したＣＯＰＹＭＯＤＥをフラグとして利用）をセットし、コピー終了後にフラグをクリアして、バックアップ側のＲＡＭへ上書きする構成とする。

【００７６】図９はコピー中にＣｈｕｒｎｅｄ－ＶＰ設定情報を受信した際の動作を示すタイミングチャートである。ＣＯＰＹＭＯＤＥは、コピー動作時に“Ｈ”となる信号である。ＣＨＵＲＮＥＤ－ＴＲは、Ｃｈｕｒｎｅｄ－ＶＰ設定情報を受信したこと示すトリガ信号であり、受信時に“Ｈ”となる。

【００７７】ＣＨＵＲＮＥＤ－ＬＴは、ＣＯＰＹＭＯＤＥが“Ｈ”で、ＣＨＵＲＮＥＤ－ＴＲが“Ｈ”になった場合にＣＨＵＲＮＥＤ－ＴＲをラッチした信号である。ＣＶＰ－ＣＴＲは、ＣＨＵＲＮＥＤ－ＬＴの立ち下がりでロードされて、バックアップ側のＲＡＭへ書き込むための書き込みアドレスを示す信号である。

【００７８】以上説明したように、コピー中に受信したＣｈｕｒｎｅｄ－ＶＰ設定情報に対しては、コピー終了後に書き込む構成とした。このように、コピーを優先して、その後に上書きすることにより、ＲＡＭへのコピー動作時のコピーエラーを防止することが可能になる。

【００７９】次にＣｈｕｒｎｅｄ－ＶＰ設定情報を受信した際の応答信号の返送制御について説明する。ＩＴＵ－Ｔ勧告Ｇ．９８３では、ＯＮＵ１０がＣｈｕｒｎｅｄ－ＶＰ設定情報を受信した場合、受信したことをＯＬＴへ通知するための応答信号を返送する旨が規定されているが、返送条件については規定されていない。

【００８０】したがって、本発明の暗号化設定情報記憶手段１１は、Ｃｈｕｒｎｅｄ－ＶＰ設定情報を受信してＲＡＭへ書き込んだ際に、再度読み出してベリファイチェック（書き込んだ値と読み出した値とを比較する）を行う。そして、正常に書き込めた場合にのみ、ＯＮＵ１０はＯＬＴへ応答信号を返送する。

【００８１】図１０は応答信号の返送制御手順を示すフローチャートである。ＲＡＭ（Ａ）をアクティブ側、ＲＡＭ（Ｂ）をバックアップ側とし、コピー動作は終了しているものとする。

【００８２】したがって、Ｃｈｕｒｎｅｄ－ＶＰ設定情報を受信した際には、ＲＡＭ（Ｂ）へ書き込み、再度ＲＡＭ（Ｂ）から読み出してベリファイチェックを行った後に応答信号の返送制御を行う。

〔Ｓ２０〕Ｃｈｕｒｎｅｄ－ＶＰ設定情報を受信する。
〔Ｓ２１〕Ｃｈｕｒｎｅｄ－ＶＰ設定情報が示すアドレスのデータをＲＡＭ（Ｂ）から読み出す。すなわち、ＶＰＩ〔１１：４〕のアドレスに対応するデータのＶＰＩ〔３：０〕の位置にあるデータ（ａビット情報）をＲＡＭ（Ｂ）から読み出す。
〔Ｓ２２〕ＲＡＭ（Ｂ）から読み出したデータのパリティチェック（ＬＳＩ間同士のデータ伝送などでは、データ送受信の信頼性確保のため、誤り訂正を行う必要があり、誤り訂正符号をデータに付加して送受信を行っている）を行う。正常の場合はステップＳ２３へ行く。パリティエラーの場合はステップＳ２９へ行く。
〔Ｓ２３〕ＲＡＭ（Ｂ）から読み出したデータと、受信したＣｈｕｒｎｅｄ－ＶＰ設定情報のａビット情報とを比較する。値が異なる場合はステップＳ２４へ行き、値が同じ場合はステップＳ２５へ行く。
〔Ｓ２４〕ステップＳ２１と同じアドレスへ、更改されたａビット情報を書き込む。
〔Ｓ２５〕ステップＳ２１と同じアドレスからデータを再び読み出す。
〔Ｓ２６〕ＲＡＭ（Ｂ）から読み出したデータのパリティチェックを行う。正常ならばステップＳ２７へ行く。パリティエラーの場合はステップＳ２９へ行く。
〔Ｓ２７〕ＲＡＭ（Ｂ）から読み出したデータと、受信したＣｈｕｒｎｅｄ－ＶＰ設定情報のａビット情報とを比較する。値が同じ場合はステップＳ２８へ行き、値が異なる場合はステップＳ２９へ行く。
〔Ｓ２８〕ＲＡＭ（Ｂ）へ正常に書き込めたので、Ｃｈｕｒｎｅｄ－ＶＰ設定情報を受信したことを通知するための応答信号をＯＬＴへ返送する。
〔Ｓ２９〕ＯＮＵ１０の全体制御を行っている全体制御部へエラー通知を送信する。
【００８３】以上説明したように、本発明の暗号化設定情報記憶手段１１は、Ｃｈｕｒｎｅｄ－ＶＰ設定情報を受信し、ＲＡＭへ書き込んだ際に正常に書き込めた否かを検証する。そして、ＯＮＵ１０は、正常に書き込めた場合にのみ応答信号を返送する構成とした。これにより、ＯＬＴ側とのＣｈｕｒｎｅｄ－ＶＰ設定情報の設定不一致を防止することが可能になる。
【００８４】次に外部記憶制御手段１３について説明する。本発明のＯＮＵ１０ではバックアップ電源を有しており、外部記憶制御手段１３は、電源断時にはバックアップ電源を利用して、Ｃｈｕｒｎｅｄ－ＶＰ設定情報を不揮発性メモリ（フラッシュメモリなど）１３ａに記憶させる。
【００８５】これにより、電源断になっても不揮発性メモリ１３ａにＣｈｕｒｎｅｄ－ＶＰ設定情報を保持することができるので、電源復旧後に再度Ｃｈｕｒｎｅｄ－ＶＰ設定情報をＯＬＴから送信要求しなくてもよい。
【００８６】また、外部記憶制御手段１３は、一旦、不揮発性メモリ１３ａにＣｈｕｒｎｅｄ－ＶＰ設定情報を格納した後は、あらたに受信したＣｈｕｒｎｅｄ－ＶＰ設定情報と、バックアップ側のＲＡＭに格納されているＣｈｕｒｎｅｄ－ＶＰ設定情報とを比較し、異なるＣｈｕｒｎｅｄ－ＶＰ設定情報のみを不揮発性メモリ１３ａに記憶させる。
【００８７】具体的には、図１０のステップＳ２４で、更改されたａビット情報を書き込んだ際に、ａビット情報が更改されていることを示す更改フラグを暗号化設定情報記憶手段１１がセットする。
【００８８】外部記憶制御手段１３は、この更改フラグが立っている場合に、バックアップ側のＲＡＭから、対応するアドレスのデータを読み出し、不揮発性メモリ１３ａへ記憶させる。このように、更改されたＣｈｕｒｎｅｄ－ＶＰ設定情報だけを記憶していくので効率よく不揮発性メモリ１３ａに記憶させることができる。
【００８９】一方、不揮発性メモリ１３ａには書き込み回数が制限されているものが多いため、さらに書き込み回数を削減する工夫が必要である。したがって、外部記憶制御手段１３では、電源復旧時にはＣｈｕｒｎｅｄ－ＶＰ設定情報を例えばＳＲＡＭ（Static-RAM）等のメモリに一旦記憶させ、電源断時にＳＲＡＭから不揮発性メモリ１３ａへ、一括してＣｈｕｒｎｅｄ－ＶＰ設定情報記憶させてもよい。これにより、不揮発性メモリ１３ａへのアクセス回数を削減することが可能になる。
【００９０】また、一旦ＳＲＡＭから不揮発性メモリ１３ａへ一括書き込みを行った初期動作以降は、更改フラグが立っているＣｈｕｒｎｅｄ－ＶＰ設定情報のみをＳＲＡＭへ書き込む。そして、電源断時にはＳＲＡＭから不揮発性メモリ１３ａへ、更改されたＣｈｕｒｎｅｄ－ＶＰ設定情報のみを記憶させてもよい。
【００９１】図１１は更改されたＣｈｕｒｎｅｄ－ＶＰ設定情報をＳＲＡＭから不揮発性メモリ１３ａへ記憶させる場合の処理手順を示すフローチャートである。
〔Ｓ３０〕暗号化設定情報記憶手段１１は、Ｃｈｕｒｎｅｄ－ＶＰ設定情報が更改されている場合は、更改フラグを立てる。
〔Ｓ３１〕外部記憶制御手段１３は、バックアップ側のＲＡＭから、更改フラグにもとづいて対応するＣｈｕｒｎｅｄ－ＶＰ設定情報を読み出す。
〔Ｓ３２〕外部記憶制御手段１３は、更改されたＣｈｕｒｎｅｄ－ＶＰ設定情報をＳＲＡＭへ書き込む。
〔Ｓ３３〕外部記憶制御手段１３は、ＯＮＵ１０の電源断時に、ＳＲＡＭが格納している情報を不揮発性メモリ１３ａへ書き込む。
【００９２】このように、電源断時には、更改されたＣｈｕｒｎｅｄ－ＶＰ設定情報のみをＳＲＡＭから不揮発性メモリ１３ａへ記憶させてもよい。これにより、不揮発性メモリ１３ａへのアクセス回数をさらに削減することが可能になる。

【００９３】次に電源復旧時のＯＮＵ１０の動作について説明する。ＩＴＵ－Ｔ勧告Ｇ．９８３では、ＯＮＵの動作状態としてｏ１状態～ｏ１０状態を定めており、特にＯＮＵの電源復旧後の状態は、ｏ１状態またはｏ９状態であることが規定されている。

【００９４】ｏ１状態とは、ＯＮＵの電源復旧後の初期状態のことである。ｏ９状態とは、緊急停止状態であり、この状態になると、ＯＮＵはネットワークから切り離されて、通信ができなくなる。

【００９５】また、本発明では、ＯＮＵ１０の電源復旧後の動作状態として、ｏ１状態へ遷移させるべきか、またはｏ９状態へ遷移させるべきかを判断するための立ち上げ準備状態（以降、ｏ０状態と呼ぶ）をあらたに設けることにした。

【００９６】本発明の暗号化設定情報記憶手段１１では、このｏ０状態を利用して、電源復旧時のｏ０状態の期間のみに、不揮発性メモリ１３ａからＣｈｕｒｎｅｄ－ＶＰ設定情報を受け付けることにする。

【００９７】これにより、ＯＮＵ１０の運用状態（以降、ｏ８状態と呼ぶ）中に、誤ってＲＡＭに対する外部からの書き込みがあった場合でもその情報を有効としないので、ＯＬＴ側とのＣｈｕｒｎｅｄ－ＶＰ設定情報の不一致を防止することが可能になる。

【００９８】一方、暗号化設定情報記憶手段１１は、ｏ０状態の時に、不揮発性メモリ１３ａから読み出されたＣｈｕｒｎｅｄ－ＶＰ設定情報と、あらたに送信された暗号化設定情報とのいずれを有効にすべきか判断して選択することができる。

【００９９】すなわち、ＯＮＵ１０は、ｏ０状態時に不揮発性メモリ１３ａから再ロードしたＣｈｕｒｎｅｄ－ＶＰ設定情報を有効にするかどうかは未定とする。なぜなら、ＯＬＴから送信される、あらたなＣｈｕｒｎｅｄ－ＶＰ設定情報をＯＮＵ１０へ設定したい（有効としたい）場合があるからである。そこで、２面あるＲＡＭのうち、一方を不揮発性メモリ１３ａからロードした値を持っておくＲＡＭ、他方をＮｏｔＣｈｕｒｎにするためにイニシャライズ（以降、ＮｏｔＣｈｕｒｎ設定と呼ぶ）をかけたＲＡＭをｏ０状態時に設定しておく。

【０１００】そして、不揮発性メモリ１３ａからロードした値を有効にしたい場合は、外部フラグをセットし、そのロードした値をＲＡＭに保持させ、その後、受信したＣｈｕｒｎｅｄ－ＶＰ設定情報をこのＲＡＭに上書きしていく。

【０１０１】また、外部フラグがセットされていない場合は、ＯＬＴからのＣｈｕｒｎｅｄ－ＶＰ設定情報を、ＮｏｔＣｈｕｒｎ設定されたＲＡＭへ書き込んでいく。それぞれの場合ともＣｈｕｒｎｉｎｇ－Ｋｅｙ更改タイミングで、コピー動作が開始される。

【０１０２】図１２は暗号化設定情報記憶手段１１の電源復旧時の動作状態を示すフローチャートである。ＲＡＭ（Ａ）をＮｏｔＣｈｕｒｎ設定されたＲＡＭとし、ＲＡＭ（Ｂ）を不揮発性メモリ１３ａからロードされたＣｈｕｒｎｅｄ－ＶＰ設定情報を保持するロード値設定ＲＡＭとする。なお、期間Ｂではユーザセルは Ｎｏｔ Ｄｅｃｈｕｒｎである。

〔Ｓ４０〕外部フラグがセットされているか否かを判断する。セットしていればステップＳ４１へ、セットしていなければステップＳ４５へ行く。

〔Ｓ４１〕ＲＡＭ（Ａ）をアクティブ側、ＲＡＭ（Ｂ）をバックアップ側と設定する。

〔Ｓ４２〕Ｃｈｕｒｎｅｄ－ＶＰ設定情報を受信した場合は、ＲＡＭ（Ｂ）へ上書きする。

〔Ｓ４３〕Ｃｈｕｒｎｉｎｇ－Ｋｅｙ更改タイミングで、ＲＡＭ（Ａ）をバックアップ側、ＲＡＭ（Ｂ）をアクティブ側に設定する。

〔Ｓ４４〕ＲＡＭ（Ｂ）の内容をＲＡＭ（Ａ）へコピーする。

〔Ｓ４５〕Ｃｈｕｒｎｅｄ－ＶＰ設定情報を受信した場合はステップＳ４６へ、受信しない場合はステップＳ４０へ戻る。

〔Ｓ４６〕ＲＡＭ（Ａ）をバックアップ側、ＲＡＭ（Ｂ）をアクティブ側と設定する。

〔Ｓ４７〕Ｃｈｕｒｎｅｄ－ＶＰ設定情報を受信した場合は、ＲＡＭ（Ａ）へ上書きする。

〔Ｓ４８〕Ｃｈｕｒｎｉｎｇ－Ｋｅｙ更改タイミングで、ＲＡＭ（Ａ）をアクティブ側、ＲＡＭ（Ｂ）をバックアップ側に設定する。

〔Ｓ４９〕ＲＡＭ（Ａ）の内容をＲＡＭ（Ｂ）へコピーする。

【０１０３】次に復号化マスク手段１４について説明する。ＯＮＵ１０ではｏ８状態になってからＤｅｃｈｕｒｎを行う。また、ｏ８状態から他の状態に遷移して、再度ｏ８状態になった時には、ＯＬＴとＯＮＵ１０のＣｈｕｒｎｉｎｇ－Ｋｅｙが一致していないと、ユーザセルに対して誤ったＤｅｃｈｕｒｎを行ってしまう可能性がある。したがって、その間は復号化処理をマスクする必要がある。図１３は復号化マスク処理を示す図である。

〔Ｓ５０〕ＯＮＵ１０がｏ８状態から、その他の状態へ遷移する。

〔Ｓ５１〕復号化マスク手段１４は、ｏ８状態からその他の状態へ遷移した時にマスクフラグをセットする。

〔Ｓ５２〕復号化マスク手段１４は、Ｄｅｃｈｕｒｎのマスクを開始する（ＮｏｔＤｅｃｈｕｒｎ）。

〔Ｓ５３〕その他の状態からｏ８状態へ遷移する。

〔Ｓ５４〕復号化マスク手段１４は、ｏ８状態になってから、最初のＣｈｕｒｎｉｎｇ－Ｋｅｙ更改タイミングを受信した場合に、マスクフラグをクリアして、Ｄｅｃｈｕｒｎのマスク解除を行う。

〔Ｓ５５〕新しいＣｈｕｒｎｉｎｇ－Ｋｅｙと新しいＣｈｕｒｎｅｄ－ＶＰ設定情報にもとづいて、Ｄｅｃｈｕ

ｒｎを行っていく。

【０１０４】このように、復号化マスク手段１４は、ｏ８状態に遷移してからＣｈｕｒｎｉｎｇ－Ｋｅｙ更改タイミングとなるまでの期間は、復号化処理をマスクしてＤｅｃｈｕｒｎをかけず、ユーザセルはすべてＮｏｔＣｈｕｒｎとする。

【０１０５】これにより、ＯＬＴとＯＮＵ１０のＣｈｕｒｎｉｎｇ－Ｋｅｙの一致を確認して初めてＤｅｃｈｕｒｎを行うことができるので、セルの誤ったＤｅｃｈｕｒｎを防止することが可能になる。

【０１０６】次に本発明の変形例について説明する。図１４はＯＮＵ１０の変形例を示す図である。なお、外部記憶制御手段１３は、上述したので説明は省略する。暗号化設定情報記憶手段１１ａは、Ｃｈｕｒｎｅｄ－ＶＰ設定情報を記憶する記憶領域を１つだけ有している。

【０１０７】暗号化情報復号化処理手段１２ａは、フレーム構成を持つ情報ストリームを受信し、暗号化設定情報記憶手段１１ａで記憶しているＣｈｕｒｎｅｄ－ＶＰ設定情報を次フレームから有効にする。そして、Ｃｈｕｒｎｅｄ－ＶＰ設定情報が示す暗号化された情報部分に対する復号化処理を次フレームから行う。

【０１０８】例えば、情報ストリーム中の１つのフレームの中で、ＶＰＩ＝“００１”（“００１”はヘキサデータ）の情報が暗号化されている旨がＣｈｕｒｎｅｄ－ＶＰ設定情報に記載されているものとする。また、ＶＰＩ＝“００１”に対応するセルがセルＣ１だとする。

【０１０９】このような暗号化設定情報を１フレーム目にＯＮＵ１０ａが受信した場合には、Ｃｈｕｒｎｅｄ－ＶＰ設定情報を暗号化設定情報記憶手段１１ａから読み出した後、次の２フレーム目からこのＣｈｕｒｎｅｄ－ＶＰ設定情報を有効にする。すなわち、２フレーム目からセルＣ１の復号化処理を行っていく。

【０１１０】このように、変形例であるＯＮＵ１０ａでは記憶領域が１つだけでよく、また、Ｃｈｕｒｎｉｎｇ－Ｋｅｙの更改時期と独立して、Ｃｈｕｒｎｅｄ－ＶＰ設定情報の有効タイミングを規定した。これにより、効率のよい復号化処理を行うことが可能になる。

【０１１１】次に本発明の光加入者線端局装置について説明する。図１５は本発明の光加入者線端局装置の原理図である。光加入者線端局装置２０は、ＡＴＭ－ＰＯＮのような光加入者系システムに接続し、暗号鍵を用いて、暗号化を行った情報部分を含む情報ストリームをＯＮＵ１０ａ～１０ｎ（総称してＯＮＵ１０）へ送信する。以降では、光加入者線端局装置２０をＯＬＴ２０と呼ぶ。

【０１１２】ＯＬＴ２０は、フラグ設定制御手段２１と、暗号化設定情報送信制御手段２２と、暗号化設定情報上書き手段２３と、暗号化設定情報更改手段２４から構成される。

【０１１３】フラグ設定制御手段２１は、情報ストリームの送信時にＯＮＵ１０の装置状態等にもとづいて、フラグを設定する。暗号化設定情報送信制御手段２２は、設定されたフラグにもとづいて、論理コネクション毎に暗号化を施したか否かを示す設定情報である暗号化設定情報（Ｃｈｕｒｎｅｄ－ＶＰ設定情報）の送信制御を行う。

【０１１４】暗号化設定情報上書き手段２３は、Ｃｈｕｒｎｅｄ－ＶＰ設定情報をＯＮＵ１０へ再度送信する上書き処理を行う。暗号化設定情報更改手段２４は、Ｃｈｕｒｎｅｄ－ＶＰ設定情報の更改タイミングを暗号化の更改周期終了時に一致させる。

【０１１５】次にフラグ設定制御手段２１の初期暗号化（以下、初期Ｃｈｕｒｎ）フラグについて説明する。ＯＬＴ２０は、停止状態から運用状態（ｏ８状態）へ遷移したＯＮＵ１０ａに対し、Ｃｈｕｒｎｅｄ－ＶＰ設定情報を送信する。ＯＮＵ１０が停止状態からｏ８状態へ遷移した時に、Ｃｈｕｒｎｅｄ－ＶＰ設定情報を送信することを初期Ｃｈｕｒｎと呼ぶ。

【０１１６】フラグ設定制御手段２１では、初期Ｃｈｕｒｎフラグを設けて、この初期Ｃｈｕｒｎを実行する。初期Ｃｈｕｒｎフラグの設定制御としては、ＯＮＵ１０が停止状態で初期Ｃｈｕｒｎフラグをクリアし（０とし）、初期Ｃｈｕｒｎ完了で初期Ｃｈｕｒｎフラグをセットする（１とする）。

【０１１７】暗号化設定情報送信制御手段２２は、ＯＮＵ１０がｏ８状態へ遷移した時に、この初期Ｃｈｕｒｎフラグをチェックし、初期Ｃｈｕｒｎフラグがセットされていなければ、初期Ｃｈｕｒｎを実行する。

【０１１８】図１６は初期Ｃｈｕｒｎフラグを用いた初期Ｃｈｕｒｎ処理手順を示すフローチャートである。なお、ＯＮＵには固有の番号ｎが与えられており、ＯＮＵの装置状態と後述する各種のフラグはｎで管理される。

〔Ｓ６０〕フラグ設定制御手段２１は、ＯＮＵ（ｎ）が停止状態の場合に初期Ｃｈｕｒｎフラグ（ｎ）を０とする。

〔Ｓ６１〕ＯＮＵ（ｎ）が停止状態からｏ８状態へ遷移する。

〔Ｓ６２〕フラグ設定制御手段２１は、ｏ８状態に遷移したＯＮＵ（ｎ）が、初期Ｃｈｕｒｎフラグ（ｎ）が０であるか否かを判断する。０ならばステップＳ６３へ行き、１ならば初期Ｃｈｕｒｎ完了とみなして終了する。

〔Ｓ６３〕暗号化設定情報送信制御手段２２は、初期Ｃｈｕｒｎを実行する。ここで、初期Ｃｈｕｒｎでは、ＯＮＵ（ｎ）に対して、４０９６ＶＰ分のＣｈｕｒｎｅｄ－ＶＰ設定情報を送信する。ＯＮＵ（ｎ）に対して、４０９６ＶＰ分のＣｈｕｒｎｅｄ－ＶＰ設定情報の送信が完了し、ＯＮＵ（ｎ）からメッセージ正常受信を通知するＡｃｋを、４０９６ＶＰ分受信すると初期Ｃｈｕｒｎは完了となり、初期Ｃｈｕｒｎフラグ（ｎ）を１とする。

【０１１９】以上説明したように、初期Ｃｈｕｒｎフラグを設けて、初期Ｃｈｕｒｎフラグを０ＮＵ１０が停止状態でクリア、初期Ｃｈｕｒｎの完了時にセットすることにした。

【０１２０】これにより、ＯＮＵ１０が停止状態からｏ８状態へ遷移した時だけに初期Ｃｈｕｒｎを実行することができ、他の状態から遷移した時には初期Ｃｈｕｒｎを実行せず、無駄な処理を省くことが可能になる。

【０１２１】次にフラグ設定制御手段２１の初期Ｃｈｕｒｎ実行中フラグについて説明する。初期Ｃｈｕｒｎを行う場合には、初期Ｃｈｕｒｎ実行中フラグを設け、初期Ｃｈｕｒｎの実行中はこの初期Ｃｈｕｒｎ実行中フラグをセットする。そして、初期Ｃｈｕｒｎ実行中フラグがセットされている場合は、次の初期Ｃｈｕｒｎ要求を受け付けないことにする。

【０１２２】すなわち、複数のＯＮＵが連続して停止状態からｏ８状態へ遷移した場合などに対し、最初に停止状態からｏ８状態へ遷移したＯＮＵに対して初期Ｃｈｕｒｎを開始し、その時に初期Ｃｈｕｒｎ実行中フラグをセットして、その他のＯＮＵは待機させる。

【０１２３】そして、実行中のＯＮＵの初期Ｃｈｕｒｎが完了すれば、待機しているＯＮＵの初期Ｃｈｕｒｎを開始していく。図１７は初期Ｃｈｕｒｎ実行中フラグを用いた初期Ｃｈｕｒｎ処理手順を示すフローチャートである。

〔Ｓ７０〕フラグ設定制御手段２１は、初期Ｃｈｕｒｎフラグ（ｎ）が０であることを確認する。

〔Ｓ７１〕フラグ設定制御手段２１は、初期Ｃｈｕｒｎ実行中フラグが０であるか否かを判断する。初期Ｃｈｕｒｎ実行中フラグが０であればステップＳ７２へ、１であればステップＳ７４へ行く。

〔Ｓ７２〕フラグ設定制御手段２１は、他のＯＮＵが初期Ｃｈｕｒｎ実行中ではないため、初期Ｃｈｕｒｎ実行中フラグを１とする。

〔Ｓ７３〕暗号化設定情報送信制御手段２２は、該当するＯＮＵ（ｎ）に対して初期Ｃｈｕｒｎを行う。

〔Ｓ７４〕暗号化設定情報送信制御手段２２は、初期Ｃｈｕｒｎ実行中フラグが０になるまで（先行する初期Ｃｈｕｒｎが終了するまで）、初期Ｃｈｕｒｎを待機する。

【０１２４】以上説明したように、初期Ｃｈｕｒｎ実行中フラグが０である場合にのみ、対応するＯＮＵに対して初期Ｃｈｕｒｎを行い、先行する初期Ｃｈｕｒｎが終了した場合に、次のＯＮＵに対して初期Ｃｈｕｒｎを行う構成とした。

【０１２５】これにより、複数のＯＮＵから連続で初期Ｃｈｕｒｎ要求が発生しても、初期ＣｈｕｒｎをＯＮＵ単位のシリアル処理として行うことができるので、複雑な輻輳処理をすることなく、効率よく初期Ｃｈｕｒｎを行うことが可能になる。

【０１２６】次にフラグ設定制御手段２１の設定更改失敗フラグについて説明する。初期Ｃｈｕｒｎが完了したＯＮＵの運用中に、ＯＬＴ２０がＣｈｕｒｎｅｄ－ＶＰ設定情報の設定更改（設定変更）や上書き処理などを行った時に、ＯＮＵ１０へのＣｈｕｒｎｅｄ－ＶＰ設定情報の設定が失敗したとする。

【０１２７】このような、Ｃｈｕｒｎｅｄ－ＶＰ設定情報の設定更改失敗（ＬＯＡｉ（Ｃｈｕｒｎ））が原因で状態落ち（停止状態へ遷移すること）が発生した場合は、再度、ｏ８状態へ遷移した時に初期Ｃｈｕｒｎを実行する必要がある。

【０１２８】そこで、フラグ設定制御手段２１では、ＯＮＵ１０の運用中にＣｈｕｒｎｅｄ－ＶＰ設定情報の設定失敗の有無を示す設定更改失敗フラグを設ける。暗号化設定情報送信制御手段２２は、設定更改失敗フラグがセットされている場合には、Ｃｈｕｒｎｅｄ－ＶＰ設定情報の設定更改に失敗したものとみなして、該当するＯＮＵ１０に対して初期Ｃｈｕｒｎを実行する。

【０１２９】なお、以降の説明では、初期Ｃｈｕｒｎが完了した運用中のＯＮＵに対して、Ｃｈｕｒｎｅｄ－ＶＰ設定情報の更改を行う場合の処理を、設定更改Ｃｈｕｒｎと呼ぶ。

【０１３０】図１８は設定更改失敗フラグを用いた初期Ｃｈｕｒｎ処理手順を示すフローチャートである。

〔Ｓ８０〕フラグ設定制御手段２１は、Ｃｈｕｒｎｅｄ－ＶＰ設定情報を送信した後、例えば、３００ｍｓ以内にＯＮＵ（ｎ）からメッセージ正常受信を示すＡｃｋを受信しない場合、設定失敗とみなして、設定更改失敗フラグ（ｎ）を１にする。

〔Ｓ８１〕暗号化設定情報送信制御手段２２は、ＯＮＵ（ｎ）に対する各種メッセージの送信を中断する。ＯＮＵ（ｎ）は停止状態となる。

〔Ｓ８２〕暗号化設定情報送信制御手段２２は、設定更改失敗フラグ（ｎ）が１となっているＯＮＵ（ｎ）が、再度ｏ８状態に遷移した時に、あらためて初期Ｃｈｕｒｎを実行する。

【０１３１】以上説明したように、ＯＮＵ１０に対して設定更改Ｃｈｕｒｎが失敗した場合には、設定更改失敗フラグを１として、再度初期Ｃｈｕｒｎを行う構成とした。これにより、設定更改Ｃｈｕｒｎの失敗時に、再度初期Ｃｈｕｒｎを行って、Ｃｈｕｒｎｅｄ－ＶＰ設定情報を送信できるので、ＯＬＴ２０とＯＮＵ１０とのＣｈｕｒｎｅｄ－ＶＰ設定情報の設定不一致を防止することが可能になる。

【０１３２】次にフラグ設定制御手段２１の設定更改未完了フラグについて説明する。初期Ｃｈｕｒｎを完了したＯＮＵ１０が、設定更改Ｃｈｕｒｎ失敗以外の何らかの要因で状態落ちした場合には、Ｃｈｕｒｎｅｄ－ＶＰ設定情報の設定更改が終了していないことになる。　そこで、フラグ設定制御手段２１では、設定更改未完了フ

ラグを設け、終了していない場合は、設定更改未完了フラグをセットする。

【０１３３】そして、暗号化設定情報送信制御手段２２は、該当するＯＮＵが再度ｏ８状態へ遷移した時に、設定更改未完了フラグをチェックし、フラグがセットされていれば初期Ｃｈｕｒｎを実行する。

【０１３４】図１９は設定更改未完了フラグを用いた初期Ｃｈｕｒｎ処理手順を示すフローチャートである。

〔Ｓ９０〕ＯＮＵ（ｎ）が状態落ちした場合は、設定更改が未完了であることを示す設定更改未完了フラグ（ｎ）を１とする。

〔Ｓ９１〕暗号化設定情報送信制御手段２２は、ＯＮＵ（ｎ）に対する各種メッセージの送信を中断する。ＯＮＵ（ｎ）は停止状態となる。

〔Ｓ９２〕暗号化設定情報送信制御手段２２は、設定更改未完了フラグ（ｎ）が１となっているＯＮＵ（ｎ）が、再度ｏ８状態に遷移した時に、あらためて初期Ｃｈｕｒｎを実行する。

【０１３５】以上説明したように、ＯＮＵ１０の状態落ちが発生した場合には、設定更改未完了フラグを１として、再度初期Ｃｈｕｒｎを行う構成とした。これにより、設定更改Ｃｈｕｒｎ失敗以外の場合でも、再度初期Ｃｈｕｒｎを行って、Ｃｈｕｒｎｅｄ－ＶＰ設定情報を送信できるので、ＯＬＴ２０とＯＮＵ１０とのＣｈｕｒｎｅｄ－ＶＰ設定情報の設定不一致を防止することが可能になる。

【０１３６】次にフラグ設定制御手段２１のＣｈｕｒｎ更改中フラグについて説明する。Ｃｈｕｒｎ更改周期の期間中に、設定更改Ｃｈｕｒｎ等（上書き処理も含め）を行うと、Ｃｈｕｒｎ更改と設定更改Ｃｈｕｒｎが輻輳する可能性があり、設定更改Ｃｈｕｒｎが正常に行われない場合がある。

【０１３７】したがって、フラグ設定制御手段２１は、Ｃｈｕｒｎ更改フラグを設け、Ｃｈｕｒｎ更改周期中はこのフラグをセットする。Ｃｈｕｒｎ更改中フラグがセットしている期間（ＯＬＴ２０から送信されるメッセージの送信禁止期間となる）に、ＯＮＵ１０からＣｈｕｒｎｅｄ－ＶＰ設定情報の更改要求等があった場合は、要求をｗａｉｔさせ、Ｃｈｕｒｎ更改終了後に設定更改Ｃｈｕｒｎを実行する。これにより、ＯＬＴ２０とＯＮＵ１０とのＣｈｕｒｎｅｄ－ＶＰ設定情報の設定不一致を防止することが可能になる。

【０１３８】次にフラグ設定制御手段２１の設定更改要求フラグについて説明する。初期Ｃｈｕｒｎが完了した運用中のＯＮＵに対し、ＯＬＴ２０が設定更改Ｃｈｕｒｎを行う場合は、外部の保守端末装置よりＯＮＵ単位に設定更改要求フラグをＯＬＴ２０にセットする。

【０１３９】ＯＬＴ２０は、設定更改要求フラグがセットされたＯＮＵに対し、設定更改Ｃｈｕｒｎを行う。設定更改Ｃｈｕｒｎ完了で設定更改要求フラグをクリアする。これにより、初期Ｃｈｕｒｎで設定したＣｈｕｒｎｅｄ－ＶＰ設定情報をｏ８状態中に更改することが可能になる。

【０１４０】一方、設定更改要求フラグは、ＯＮＵ単位とし、１回の設定更改で１ＯＮＵにつき１ＶＰＩの更改に制限する。このため、同報のＶＰＩの設定更改の場合には、すべてのＯＮＵに対し同一設定ができる。

【０１４１】また、１ＯＮＵにつき１ＶＰＩと制限することで、１回の設定更改Ｃｈｕｒｎは、Ｃｈｕｒｎ更改周期内で完了できるため、Ｃｈｕｒｎ設定更改処理時間を明確に規定できる。

【０１４２】次にフラグ設定制御手段２１の設定更改実行中フラグについて説明する。設定更改Ｃｈｕｒｎは、Ｃｈｕｒｎｅｄ－ＶＰ設定情報の設定更改処理であるため処理の優先順位が高い。そこで設定更改実行中フラグを設け、実行中はこのフラグをセットする。

【０１４３】設定更改実行中フラグのセット中は、他のＯＮＵからの要求をｗａｉｔさせることで割り込みを防止し、Ｃｈｕｒｎ設定更改の処理の優先順位を高くする。次に設定更改Ｃｈｕｒｎの処理手順について図２０～図２３を用いて説明する。図２０、図２１は設定更改Ｃｈｕｒｎ開始時の処理手順を示すフローチャートである。

〔Ｓ１００〕暗号化設定情報送信制御手段２２は、設定更改要求フラグが１か否かを判断する（配下のＯＮＵ１０ａ～１０ｎの１ＯＮＵでも設定更改要求があるか否かを判断する）。１ならばステップＳ１０１へ、０ならば終了する。

〔Ｓ１０１〕暗号化設定情報送信制御手段２２は、ＳＥＮＤフラグ（フラグ設定制御手段２１は、ＯＬＴ２０がＣｈｕｒｎｅｄ－ＶＰ設定情報を送信している場合は、ＳＥＮＤフラグをセットする）をチェックする。

【０１４４】ＳＥＮＤフラグが１であれば０になるまで待機し（ステップＳ１０１を繰り返す）、ＳＥＮＤフラグが０ならステップＳ１０２へ行く。

〔Ｓ１０２〕フラグ設定制御手段２１は、ＳＥＮＤフラグをあらためて１にセットして、その他の要求を受け付けないようにする。

【０１４５】ここで、ステップＳ１０３以降から並列処理となる。例えば、ＯＮＵ１０ａ、１０ｂ及び１０ｃに対して設定更改要求があったものとすると、ＯＮＵ１０ａ、１０ｂ及び１０ｃの３つの並列処理が行われる。以降では、ＯＮＵ１０ａに対する設定更改Ｃｈｕｒｎの処理を説明する。

〔Ｓ１０３〕フラグ設定制御手段２１は、設定更改要求フラグを０にする。

〔Ｓ１０４〕フラグ設定制御手段２１は、設定更改実行中フラグを１にする。

〔Ｓ１０５〕暗号化設定情報送信制御手段２２は、Ｃｈｕｒｎｅｄ－ＶＰ設定情報に更改ＶＰＩをセットし、Ｃ

ｈｕｒｎｅｄ－ＶＰ設定情報の送信回数ｋ（例えば、ｋ＝３）を設定する。

〔Ｓ１０６〕暗号化設定情報送信制御手段２２は、Ｃｈｕｒｎ更改中フラグが１か否かを判断する。１の場合は０になるまで待機し（ステップＳ１０７を繰り返す）、０の場合はステップＳ１０７へ行く。

〔Ｓ１０７〕ＯＮＵ１０ａがｏ８状態から状態落ちしたか否かを判断する。すなわち、設定更改未完了フラグをチェックし、フラグが１ならばステップＳ１１０へ行き、フラグが０ならステップＳ１０８へ行く。

〔Ｓ１０８〕暗号化設定情報送信制御手段２２は、Ｃｈｕｒｎｅｄ－ＶＰ設定情報を送信し、Ｃｈｕｒｎｅｄ－ＶＰ設定情報を１回送信する度にｋから１をデクリメント（ｋ＝ｋ－１）し、送信回数を管理する。

〔Ｓ１０９〕ｋ＝０なら終了し、ｋ≠０ならステップＳ１０６へ戻る。

〔Ｓ１１０〕暗号化設定情報送信制御手段２２は、初期Ｃｈｕｒｎを行う。

【０１４６】図２２はＡＣＫメッセージの受信処理時のフローチャートを示す図である。ＯＬＴ２０がＣｈｕｒｎｅｄ－ＶＰ設定情報を送信した場合、ＯＮＵ１０ａが正常にＣｈｕｒｎｅｄ－ＶＰ設定情報を受信すると、ＡＣＫメッセージをＯＬＴ２０へ返送する。

〔Ｓ１２０〕暗号化設定情報送信制御手段２２からＣｈｕｒｎｅｄ－ＶＰ設定情報の送信後（例えば、３回送信した後）、一定時間内（例えば、３００ｍｓ以内）でＡＣＫメッセージの返答があるか計測する。タイムアウトした場合はステップＳ１２３へ、そうでなければステップＳ１２１へ行く。

〔Ｓ１２１〕Ｃｈｕｒｎ更改中フラグが１か否かを判断する。１の場合は０になるまで待機し（ステップＳ１２１を繰り返す）、０の場合はステップＳ１２２へ行く。

〔Ｓ１２２〕フラグ設定制御手段２１は、設定更改実行中フラグを０にする。そして、有効となるＣｈｕｒｎｅｄ－ＶＰ設定情報を送信する。

〔Ｓ１２３〕フラグ設定制御手段２１は、設定更改失敗フラグを１にする。

〔Ｓ１２４〕暗号化設定情報送信制御手段２２は、初期Ｃｈｕｒｎを行う。

【０１４７】図２３は設定更改Ｃｈｕｒｎ終了時のフローチャートを示す図である。

〔Ｓ１３０〕すべてのＯＮＵの設定更改実行中フラグを監視し、設定更改実行中フラグがすべて０ならば、処理完了となりステップＳ１３１へ行く。そうでなければ０になるまで設定更改実行中フラグを監視し続ける（ステップＳ１３０を繰り返す）。

〔Ｓ１３１〕ＳＥＮＤフラグを０にして、他の処理に解放する。

【０１４８】次に暗号化設定情報上書き手段２３について説明する。初期Ｃｈｕｒｎ完了後、Ｃｈｕｒｎｅｄ－ＶＰ設定情報の設定更改がなければ、その後、ＯＬＴ２０がＯＮＵ１０に対してＣｈｕｒｎｅｄ－ＶＰ設定情報を送信することはない。

【０１４９】このため、従来では何らかの原因で、ＯＬＴ２０とＯＮＵ１０とのＣｈｕｒｎｅｄ－ＶＰ設定情報が設定不一致となった場合でも不一致となった状態を確認することができなかった。

【０１５０】そこで、本発明では暗号化設定情報上書き手段２３を設け、ＯＮＵ１０が運用中、初期Ｃｈｕｒｎ完了をトリガとして、Ｃｈｕｒｎｅｄ－ＶＰ設定情報の上書き処理である上書きＣｈｕｒｎを実行させることにした。これにより、何らかの原因でＯＬＴ２０とＯＮＵ１０とのＣｈｕｒｎｅｄ－ＶＰ設定情報が設定不一致となった場合でも、上書きＣｈｕｒｎで一致させることができる。

【０１５１】また、上書きＣｈｕｒｎは、ＯＬＴ２０とＯＮＵ１０とのＣｈｕｒｎｅｄ－ＶＰ設定情報を一致させるための保護機能であるため、処理の優先順位は低くて構わない。

【０１５２】そこで、上書きＣｈｕｒｎのＣｈｕｒｎｅｄ－ＶＰ設定情報に対する送信要求は、他のメッセージ送信要求がある場合や設定更改Ｃｈｕｒｎを行っている等の場合はｗａｉｔさせて、上書きＣｈｕｒｎの優先順位を低くする。これにより、他のメッセージ送信を圧迫せずに、上書きＣｈｕｒｎを実行できる。

【０１５３】さらに、暗号化設定情報上書き手段２３の内部には、上書きＣｈｕｒｎを実行するためのタイマが設けられる。このタイマは、上書きＣｈｕｒｎ用のＣｈｕｒｎｅｄ－ＶＰ設定情報の送信後に起動し、上書きＣｈｕｒｎを行うべき最低限の周期を計測する。

【０１５４】そして、タイマで計測された次の送信時刻（他のメッセージ送信と競合しないように設定される）がくるまでは、上書きＣｈｕｒｎ用のＣｈｕｒｎｅｄ－ＶＰ設定情報は送信しない。

【０１５５】また、タイマの設定周期は、保守端末装置を通じて、任意の値を設定できる。したがって、上書きＣｈｕｒｎ設定に柔軟性を持たせることができる。次にＣｈｕｒｎｉｎｇ－ＫｅｙアップデートメッセージとＣｈｕｒｎｅｄ－ＶＰ設定情報との送信時の競合防止について説明する。

【０１５６】ＩＴＵ－Ｔ勧告Ｇ．９８３では、ＯＮＵ１０へのメッセージは、一定周期に発生する下りＰＬＯＡＭセルにより送信される。したがって、ＰＬＯＡＭセル周期で送信すべきメッセージの調停処理を行って、ＯＮＵ１０へ送信するメッセージを決定しなければならない。

【０１５７】Ｃｈｕｒｎｉｎｇ－ＫｅｙアップデートメッセージはＩＴＵ－Ｔ勧告Ｇ．９８３では、図５で上述したように１６×Ｔフレーム間隔で送信される。また、Ｃｈｕｒｎｅｄ－ＶＰ設定情報は、Ｃｈｕｒｎ更改中フラグがセットされていない間

で、３回の送信を完了する必要がある。

【０１５８】暗号化設定情報送信制御手段２２は、Ｃｈｕｒｎｉｎｇ－Ｋｅｙアップデートメッセージと、Ｃｈｕｒｎｅｄ－ＶＰ設定情報との調停処理を行った場合には、Ｃｈｕｒｎｉｎｇ－Ｋｅｙアップデートメッセージを優先する。

【０１５９】すると、Ｃｈｕｒｎｉｎｇ－Ｋｅｙアップデートメッセージは、１６×Ｔフレーム間隔に自動的に送信される。その後、Ｃｈｕｒｎｅｄ－ＶＰ設定情報が例えば１６×Ｔフレーム間隔で３回自動的に送信される。

【０１６０】すなわち、Ｃｈｕｒｎｉｎｇ－Ｋｅｙアップデートメッセージと、Ｃｈｕｒｎｅｄ－ＶＰ設定情報の初回のみが調停対象となり、初回のＣｈｕｒｎｉｎｇ－Ｋｅｙアップデートメッセージが送信されれば２回目、３回目のメッセージ送信は互いに競合を起こすことなく自動的に送信することが可能になる。

【０１６１】次に暗号化設定情報更改手段２４について説明する。ＩＴＵ－Ｔ勧告Ｇ．９８３では、Ｃｈｕｒｎｉｎｇ－Ｋｅｙ更改タイミングは規定されているが、Ｃｈｕｒｎｅｄ－ＶＰ設定情報の更改タイミングは規定されていない。このため、ＯＬＴ２０ではＣｈｕｒｎｅｄ－ＶＰ設定情報に対して、不規則に設定情報の更改を行うと、ＯＬＴ２０とＯＮＵ１０とのＣｈｕｒｎｅｄ－ＶＰ設定情報の設定不一致を起こしてしまう可能性がある。

【０１６２】そこで、暗号化設定情報更改手段２４は、Ｃｈｕｒｎｉｎｇ－Ｋｅｙ更改タイミングでＣｈｕｒｎｅｄ－ＶＰ設定情報の更改を行うことにして不一致を防止する。

【０１６３】図２４はＣｈｕｒｎｅｄ－ＶＰ設定情報の更改を示す図である。Ｃｈｕｒｎｅｄ－ＶＰ設定情報を３回送信完了後の最初のＣｈｕｒｎｉｎｇ－Ｋｅｙ更改タイミングｔで、送信されたＣｈｕｒｎｅｄ－ＶＰ設定情報に対する設定更改を行っていく。

【０１６４】これにより、ＯＬＴ２０とＯＮＵ１０間でＣｈｕｒｎｅｄ－ＶＰ設定情報の設定更改を同期して行うことが可能になり、Ｃｈｕｒｎｅｄ－ＶＰ設定情報の設定不一致を防止することが可能になる。

【０１６５】

【発明の効果】以上説明したように、本発明の光加入者線終端装置は、現在使用中の暗号化設定情報を記憶するアクティブ側の第１の記憶手段と、新しく更改された暗号化設定情報を記憶するバックアップ側の第２の記憶手段との切り替え制御を行い、読み出した暗号化設定情報にもとづいて、次フレームの先頭から暗号化された情報部分の復号化処理を行う構成とした。これにより、暗号化設定情報の送信側と受信側との暗号化・復号化の処理タイミングのずれを防止し、高品質な通信制御を行うことが可能になる。

【０１６６】また、本発明の光加入者線端局装置は、受信装置へ情報ストリームを送信する際に、フラグの設定制御を行い、フラグにもとづいて、暗号化設定情報の送信制御を行う構成とした。これにより、暗号化設定情報の送信側と受信側との暗号化・復号化の処理タイミングのずれを防止し、高品質な通信制御を行うことが可能になる。

【図面の簡単な説明】

【図１】本発明の光加入者線終端装置の原理図である。

【図２】情報ストリームの構成及びＣｈｕｒｎｅｄ－ＶＰ設定情報のフォーマットを示す図である。

【図３】次フレームでＤｅｃｈｕｒｎを実現するためのブロック構成を示す図である。

【図４】次フレームからＤｅｃｈｕｒｎを行う際のタイミングチャートを示す図である。

【図５】Ｃｈｕｒｎｉｎｇ－Ｋｅｙの更改シーケンスを示す図である。

【図６】２面ＲＡＭを持つＯＮＵのブロック構成を示す図である。

【図７】コピー動作手順を示すフローである。

【図８】コピー動作時のタイミングチャートを示す図である。

【図９】コピー中にＣｈｕｒｎｅｄ－ＶＰ設定情報を受信した際の動作を示すタイミングチャートである。

【図１０】応答信号の返送制御手順を示すフローチャートである。

【図１１】更改されたＣｈｕｒｎｅｄ－ＶＰ設定情報をＳＲＡＭから不揮発性メモリへ記憶させる場合の処理手順を示すフローチャートである。

【図１２】暗号化設定情報記憶手段の電源復旧時の動作状態を示すフローチャートである。

【図１３】復号化マスク処理を示す図である。

【図１４】ＯＮＵの変形例を示す図である。

【図１５】本発明の光加入者線端局装置の原理図である。

【図１６】初期Ｃｈｕｒｎフラグを用いた初期Ｃｈｕｒｎ処理手順を示すフローチャートである。

【図１７】初期Ｃｈｕｒｎ実行中フラグを用いた初期Ｃｈｕｒｎ処理手順を示すフローチャートである。

【図１８】設定更改失敗フラグを用いた初期Ｃｈｕｒｎ処理手順を示すフローチャートである。

【図１９】設定更改未完了フラグを用いた初期Ｃｈｕｒｎ処理手順を示すフローチャートである。

【図２０】設定更改Ｃｈｕｒｎ開始時の処理手順を示すフローチャートである。

【図２１】　設定更改Ｃｈｕｒｎ開始時の処理手順を示すフローチャートである。

【図２２】ＡＣＫメッセージの受信処理時のフローチャートを示す図である。

【図２３】設定更改Ｃｈｕｒｎ終了時のフローチャート

を示す図である。

【図２４】Ｃｈｕｒｎｅｄ－ＶＰ設定情報の更改を示す図である。

【図２５】ＡＴＭ－ＰＯＮシステムの構成を示す図である。

【符号の説明】

１０　光加入者線終端装置

１１　暗号化設定情報記憶手段

１２　暗号化設定情報復号化処理手段

１３　外部記憶制御手段

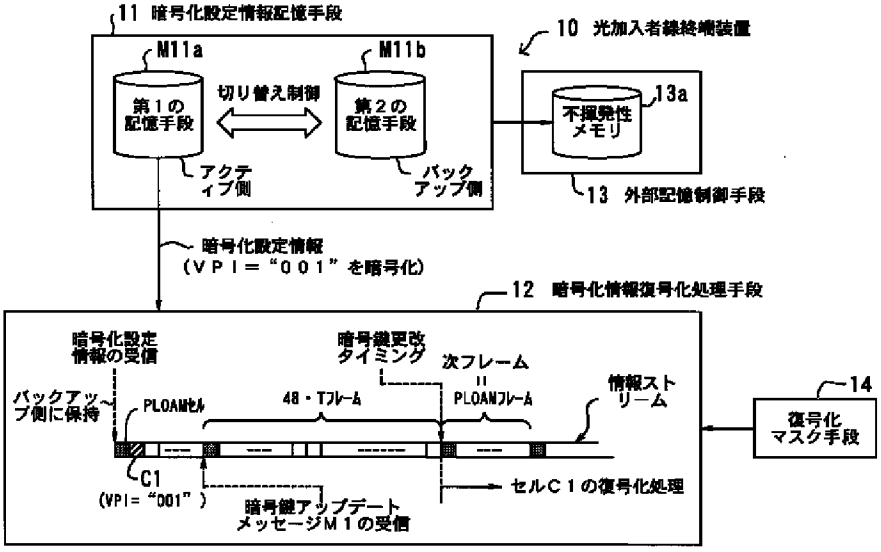
１３ａ　不揮発性メモリ

１４　復号化マスク手段

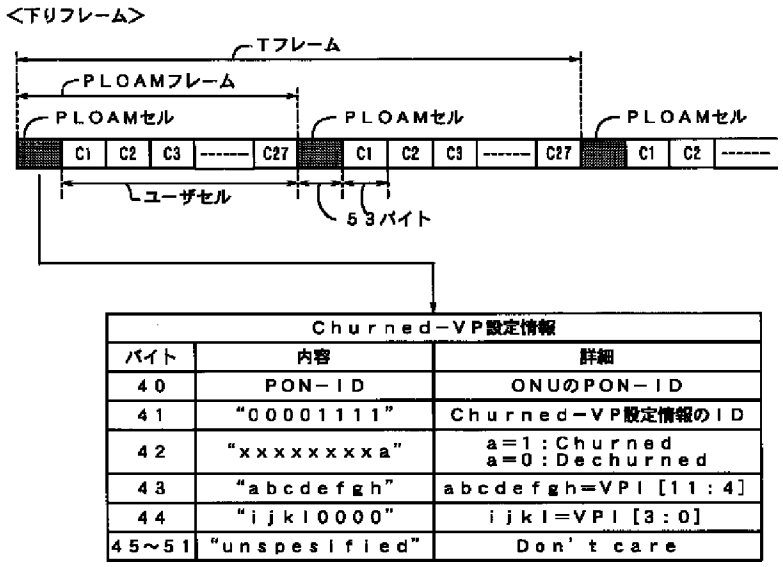
Ｍ１１ａ　第１の記憶手段

Ｍ１１ｂ　第２の記憶手段

【図１】

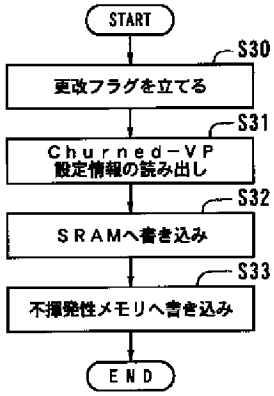


【図２】

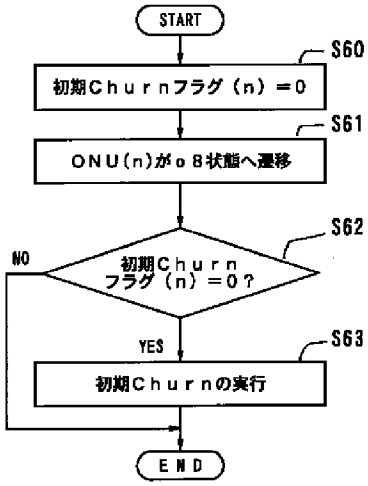


Ｃｈｕｒｎｅｄ－ＶＰ設定情報		
バイト	内容	詳細
４０	ＰＯＮ－ＩＤ	ＯＮＵのＰＯＮ－ＩＤ
４１	“００００１１１１”	Ｃｈｕｒｎｅｄ－ＶＰ設定情報のＩＤ
４２	“ｘｘｘｘｘｘｘｘａ”	ａ＝１：Ｃｈｕｒｎｅｄ ａ＝０：Ｄｅｃｈｕｒｎｅｄ
４３	“ａｂｃｄｅｆｇｈ”	ａｂｃｄｅｆｇｈ＝ＶＰＩ［１１：４］
４４	“ｉｊｋｌ０００”	ｉｊｋｌ＝ＶＰＩ［３：０］
４５～５１	“ｕｎｓｐｅｓｌｆｌｅｄ”	Ｄｏｎ’ｔ ｃａｒｅ

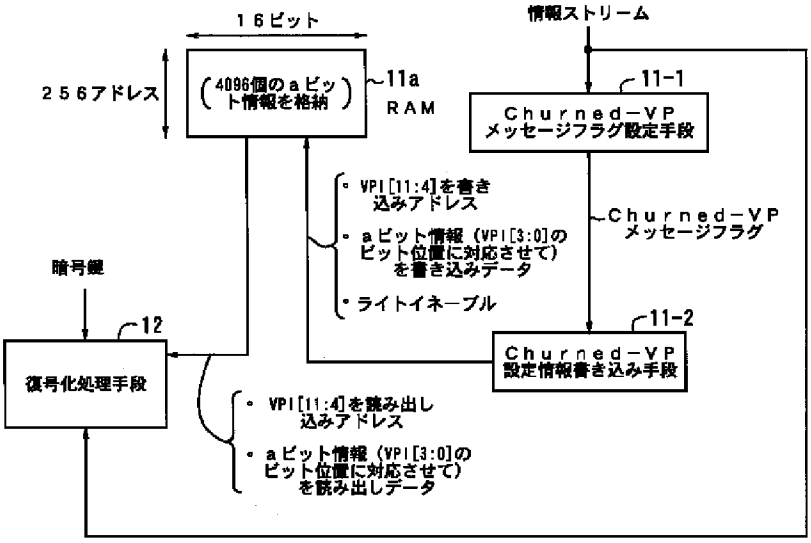
【図１１】



【図１６】

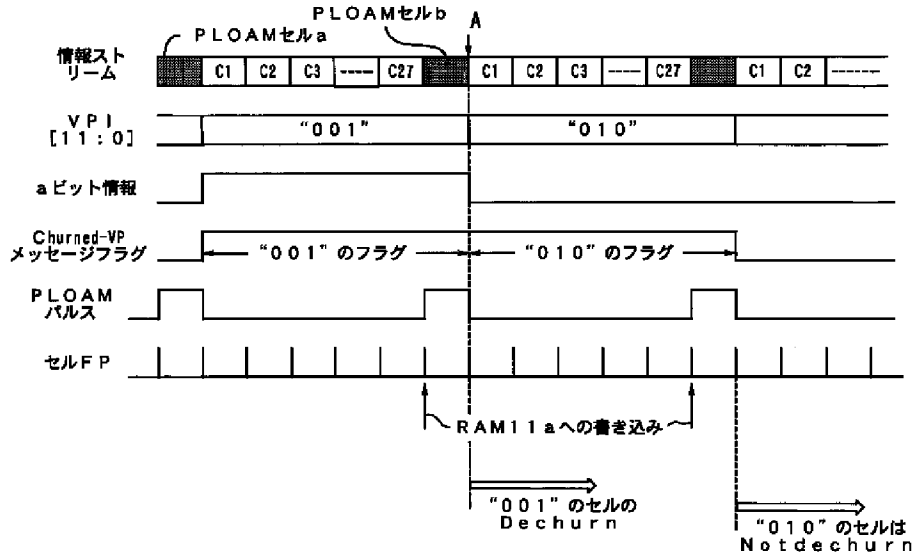


【図３】

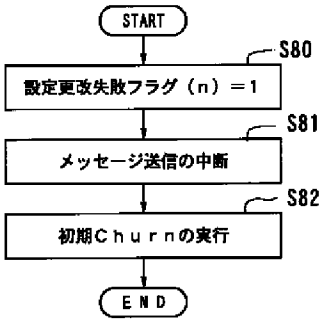


【図４】

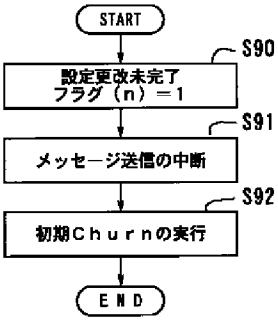
【図９】



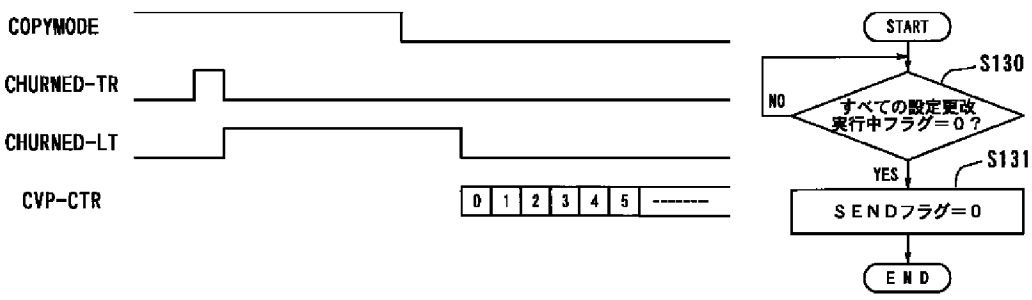
【図１８】



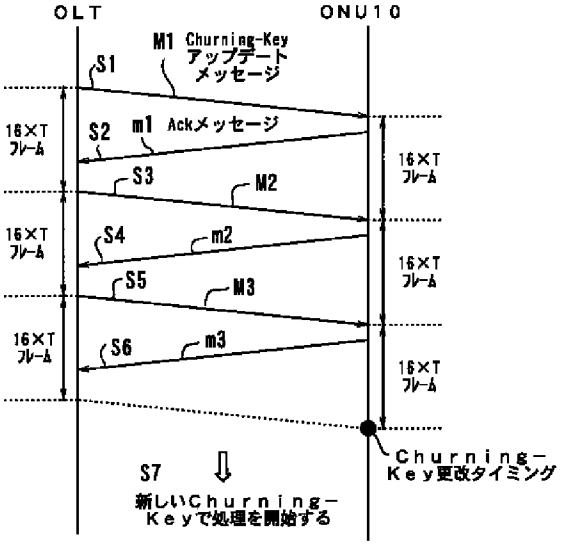
【図１９】



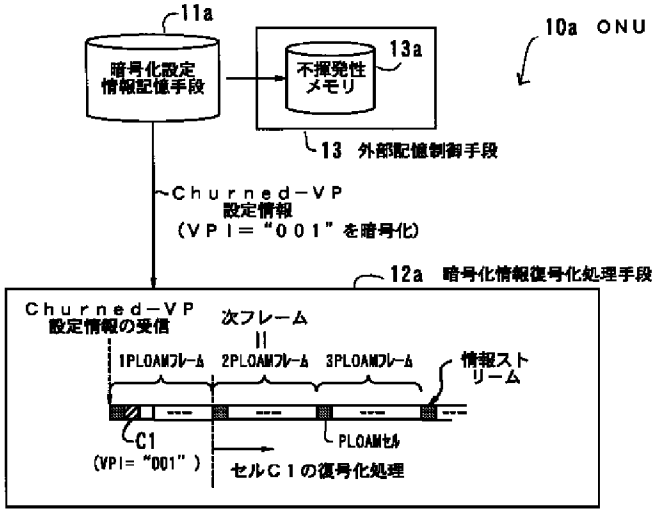
【図２３】



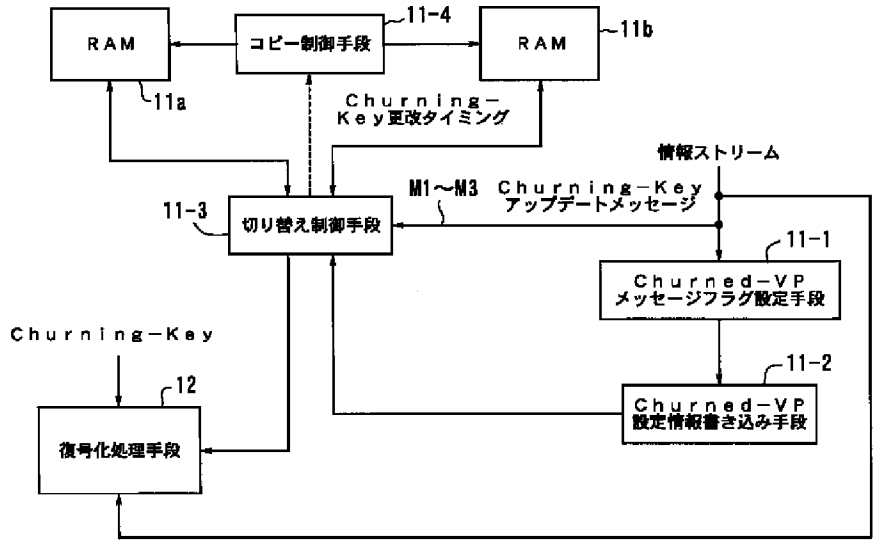
【図５】


OLT
ONU10
M1 Churning-Key アップデート メッセージ
S1
S2
m1 Ackメッセージ
S3
M2
S4
m2
S5
M3
S6
m3
16×T フレーム
S7
新しいChurning-Key で処理を開始する
Churning-Key更改タイミング

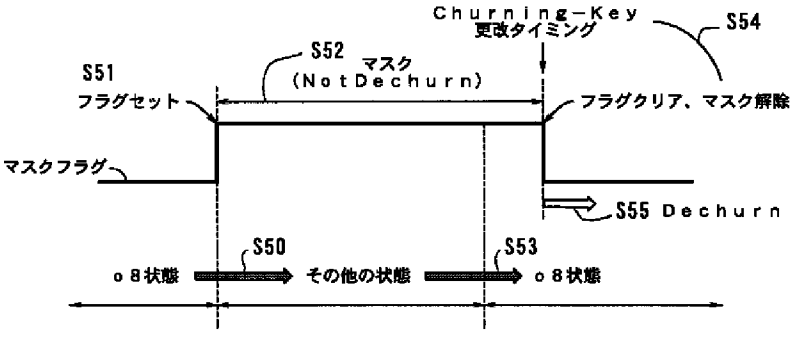
【図１４】


11a
暗号化設定 情報記憶手段
不揮発性 メモリ
13a
10a ONU
13 外部記憶制御手段
Churned-VP 設定情報 (VPI="001"を暗号化)
12a 暗号化情報復号化処理手段
Churned-VP 設定情報の受信
次フレーム
1PLOAMフレーム
2PLOAMフレーム
3PLOAMフレーム
情報ストリーム
C1
(VPI="001")
PLOAMセル
セルC1の復号化処理

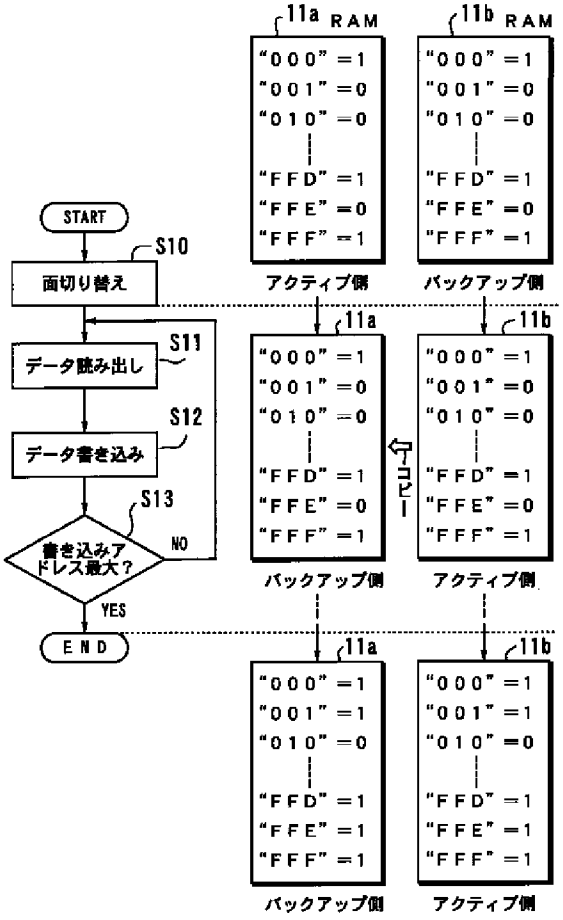
【図６】


RAM
11a
コピー制御手段
11-4
RAM
11b
Churning-Key更改タイミング
情報ストリーム
M1～M3 Churning-Key アップデートメッセージ
11-3
切り替え制御手段
11-1
Churned-VP メッセージフラグ設定手段
Churning-Key
12
復号化処理手段
11-2
Churned-VP 設定情報書き込み手段

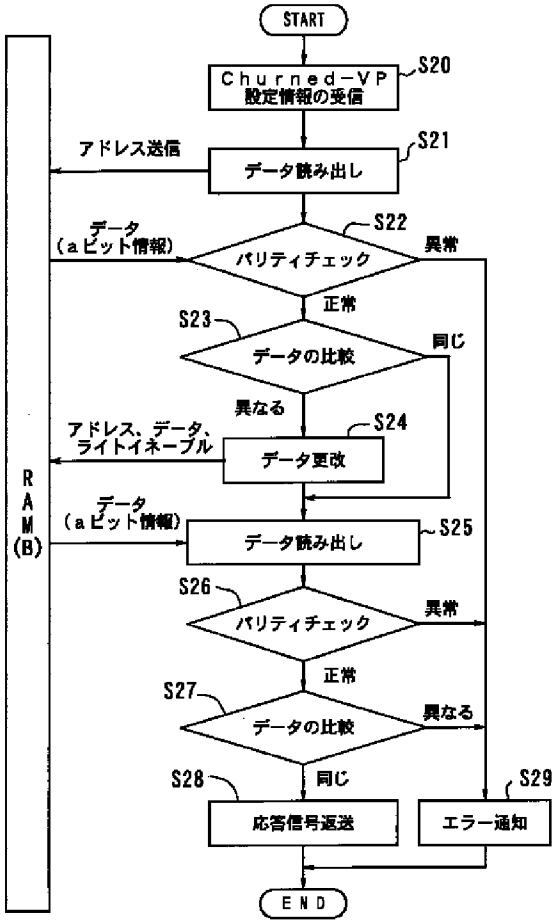
【図１３】


Churning-Key 更改タイミング
S54
S52 マスク (NotDechurn)
S51
フラグセット
フラグクリア、マスク解除
マスクフラグ
S55 Dechurn
S50
S53
o8状態
その他の状態
o8状態

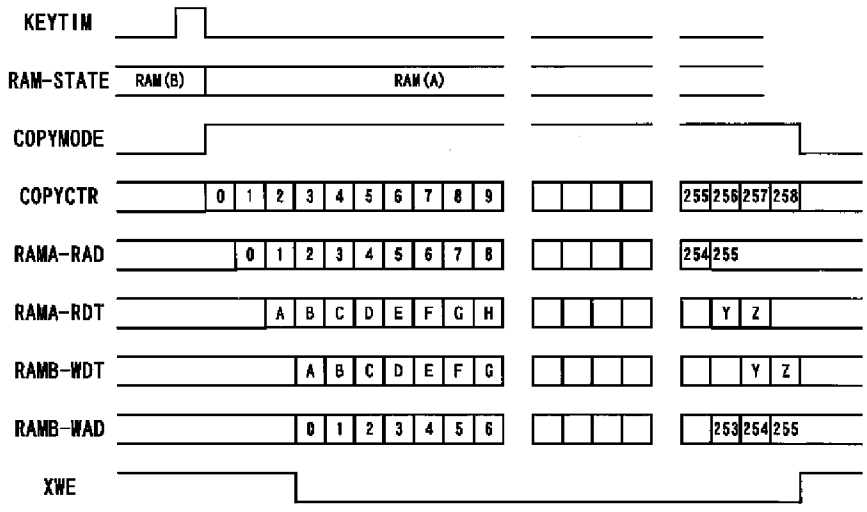
【図７】


11a RAM
11b RAM
"000"=1
"001"=0
"010"=0
"FFD"=1
"FFE"=0
"FFF"=1
アクティブ側
バックアップ側
START
S10
面切り替え
S11
データ読み出し
S12
データ書き込み
S13
書き込みアドレス最大？
NO
YES
END
コピー
"000"=1
"001"=1
"010"=0
"FFD"=1
"FFE"=1
"FFF"=1

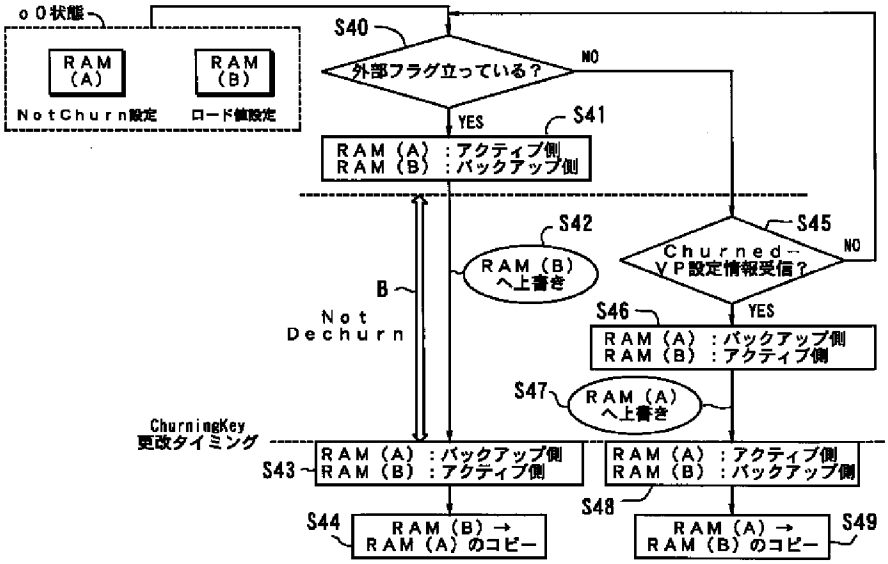
【図１０】


START
Churned-VP
設定情報の受信
S20
アドレス送信
データ読み出し
S21
データ
(aビット情報)
パリティチェック
S22
異常
正常
S23
データの比較
同じ
異なる
アドレス、データ、
ライトイネーブル
S24
データ更改
RAM(B)
データ
(aビット情報)
データ読み出し
S25
S26
パリティチェック
異常
正常
S27
データの比較
異なる
同じ
S28
応答信号返送
S29
エラー通知
END

【図８】

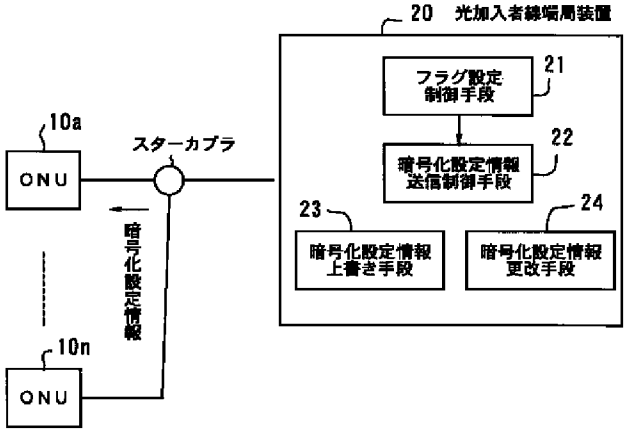

KEYTIM
RAM-STATE
RAM(B)
RAM(A)
COPYMODE
COPYCTR
0 1 2 3 4 5 6 7 8 9
255 256 257 258
RAMA-RAD
0 1 2 3 4 5 6 7 8
254 255
RAMA-RDT
A B C D E F G H
Y Z
RAMB-WDT
A B C D E F G
Y Z
RAMB-WAD
0 1 2 3 4 5 6
253 254 255
XWE

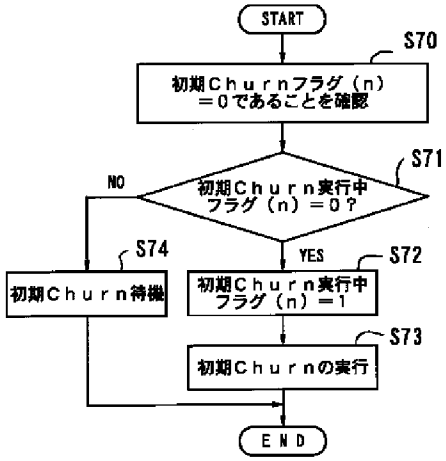
【図１２】



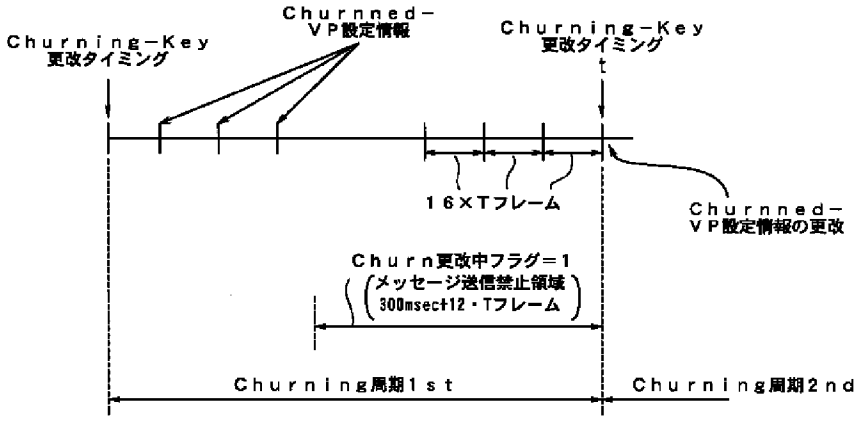
【図１５】

【図１７】

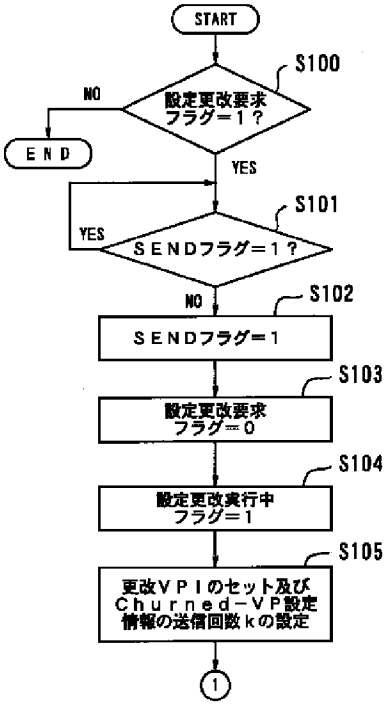




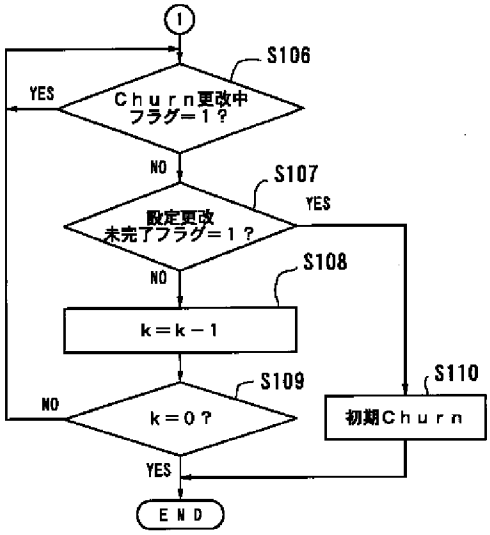
【図２４】



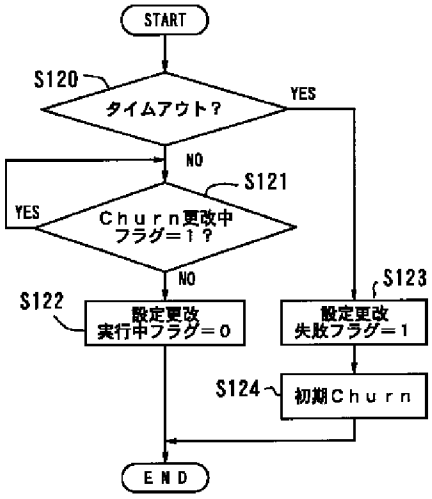
【図２０】


START
S100
設定更改要求
フラグ＝１？
NO
END
YES
S101
YES
ＳＥＮＤフラグ＝１？
NO
S102
ＳＥＮＤフラグ＝１
S103
設定更改要求
フラグ＝０
S104
設定更改実行中
フラグ＝１
S105
更改ＶＰＩのセット及び
Ｃｈｕｒｎｅｄ－ＶＰ設定
情報の送信回数ｋの設定
①

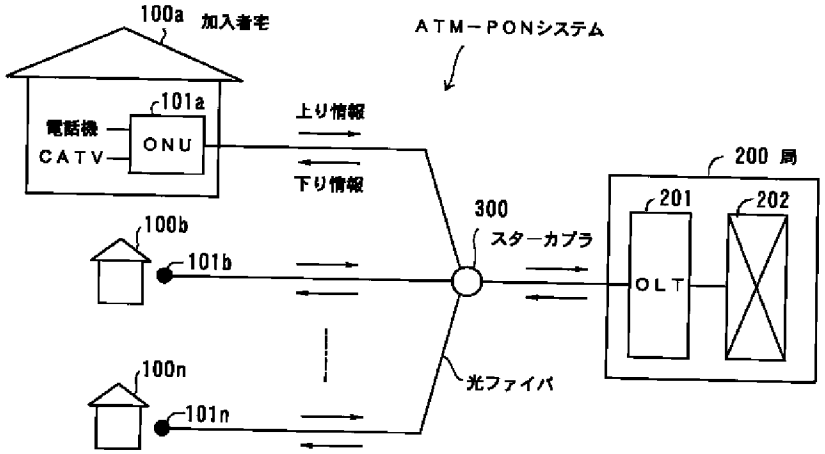
【図２１】


①
S106
YES
Ｃｈｕｒｎ更改中
フラグ＝１？
NO
S107
設定更改
未完了フラグ＝１？
YES
NO
S108
ｋ＝ｋ－１
S109
NO
ｋ＝０？
S110
初期Ｃｈｕｒｎ
YES
END

【図２２】


START
S120
タイムアウト？
YES
NO
S121
YES
Ｃｈｕｒｎ更改中
フラグ＝１？
NO
S122
設定更改
実行中フラグ＝０
S123
設定更改
失敗フラグ＝１
S124
初期Ｃｈｕｒｎ
END

【図２５】



【手続補正書】
【提出日】平成１２年２月７日（２０００．２．７）
【手続補正１】
【補正対象書類名】明細書
【補正対象項目名】全文
【補正方法】変更
【補正内容】
【書類名】　　明細書
【発明の名称】　光加入者線終端装置及び光加入者線端局装置
【特許請求の範囲】
【請求項１】　光加入者系システムに接続して情報ストリームを受信し、暗号鍵を用いて、暗号化された情報部分の復号化を行う光加入者線終端装置において、
論理コネクション毎に暗号化を施したか否かを示す設定情報である暗号化設定情報に対し、現在使用中の暗号化設定情報を記憶するアクティブ側の第１の記憶手段と、新しく更改された暗号化設定情報を記憶するバックアップ側の第２の記憶手段とを含み、前記第１の記憶手段及び前記第２の記憶手段への記憶制御を行い、前記暗号鍵の暗号鍵更改タイミングで、前記第１の記憶手段と前記第２の記憶手段との切り替え制御を行う暗号化設定情報記憶手段と、
フレーム構成を持つ前記情報ストリームを受信し、記憶している前記暗号化設定情報を、前記暗号鍵更改タイミング以後の次フレームから有効にして、前記暗号化設定情報が示す暗号化された前記情報部分に対する復号化処理を前記次フレームから行う暗号化情報復号化処理手段と、
を有することを特徴とする光加入者線終端装置。
【請求項２】　前記暗号化設定情報記憶手段は、前記暗号鍵更改タイミングで前記第１の記憶手段と前記第２の記憶手段とを切り替えた後、あらたにアクティブ側になった第１の記憶手段に記憶してある前記暗号化設定情報を、あらたにバックアップ側になった第２の記憶手段へコピーすることを特徴とする請求項１記載の光加入者線終端装置。
【請求項３】　前記暗号化設定情報記憶手段は、バックアップ側の第２の記憶手段へのコピー中に、あらたな暗号化設定情報を受信した場合は、前記コピーの終了後に前記あらたな暗号化設定情報を前記第２の記憶手段に記憶することを特徴とする請求項２記載の光加入者線終端装置。
【請求項４】　前記暗号化設定情報記憶手段は、読み出しポートが２つある前記第１の記憶手段及び前記第２の記憶手段を含むことを特徴とする請求項１記載の光加入者線終端装置。
【請求項５】　前記暗号化設定情報記憶手段は、前記暗号化設定情報を受信して、前記第１の記憶手段または前記第２の記憶手段へ正常に書き込めた否かを検証し、正常に書き込めた場合にのみ応答信号を返送することを特徴とする請求項１記載の光加入者線終端装置。
【請求項６】　前記暗号化設定情報を不揮発性メモリに記憶させる外部記憶制御手段をさらに有することを特徴とする請求項１記載の光加入者線終端装置。
【請求項７】　前記外部記憶制御手段は、受信した前記暗号化設定情報と、バックアップ側の前記第２の記憶手段に格納されている暗号化設定情報とを比較し、異なる暗号化設定情報のみ前記不揮発性メモリに記憶させることを特徴とする請求項６記載の光加入者線終端装置。
【請求項８】　前記外部記憶制御手段は、前記暗号化設定情報をメモリに記憶させ、電源断時に前記メモリから前記不揮発性メモリへ、一括して前記暗号化設定情報を

記憶させることを特徴とする請求項６記載の光加入者線終端装置。

【請求項９】　前記外部記憶制御手段は、前記暗号化設定情報をメモリに記憶させ、電源断時に前記メモリから前記不揮発性メモリへ、更改された暗号化設定情報のみ記憶させることを特徴とする請求項６記載の光加入者線終端装置。

【請求項１０】　前記暗号化設定情報記憶手段は、電源復旧時の立ち上げ準備状態の期間のみ、前記不揮発性メモリからの前記暗号化設定情報を受け付けることを特徴とする請求項６記載の光加入者線終端装置。

【請求項１１】　前記暗号化設定情報記憶手段は、電源復旧時に、前記不揮発性メモリから読み出された前記暗号化設定情報、またはあらたに送信された暗号化設定情報の一方を選択して有効にすることを特徴とする請求項６記載の光加入者線終端装置。

【請求項１２】　前記暗号化情報の復号化処理を行える運用状態から、他の状態へ遷移して、再度前記運用状態になった場合は、前記運用状態になった時から前記暗号鍵更改タイミングを受信するまでの期間の復号化処理をマスクする復号化マスク手段をさらに有することを特徴とする請求項１記載の光加入者線終端装置。

【請求項１３】　光加入者系システムに接続して情報ストリームを受信し、暗号鍵を用いて、暗号化された情報部分の復号化を行う光加入者線終端装置において、
論理コネクション毎に暗号化を施したか否かを示す設定情報である暗号化設定情報を記憶する暗号化設定情報記憶手段と、
フレーム構成を持つ前記情報ストリームを受信し、記憶している前記暗号化設定情報を次フレームから有効にして、前記暗号化設定情報が示す暗号化された前記情報部分に対する復号化処理を前記次フレームから行う暗号化情報復号化処理手段と、
を有することを特徴とする光加入者線終端装置。

【請求項１４】　光加入者系システムに接続して、暗号鍵を用いて暗号化を行った情報部分を含む情報ストリームを送信する光加入者線端局装置において、
受信装置へ前記情報ストリームを送信する際に、フラグの設定制御を行うフラグ設定制御手段と、
前記フラグにもとづいて、論理コネクション毎に暗号化を施したか否かを示す設定情報である暗号化設定情報の送信制御を行う暗号化設定情報送信制御手段と、
を有することを特徴とする光加入者線端局装置。

【請求項１５】　前記フラグ設定制御手段は、初期暗号化フラグを有し、前記初期暗号化フラグを前記受信装置が停止状態でクリア、初期暗号化の完了時にセットすることを特徴とする請求項１４記載の光加入者線端局装置。

【請求項１６】　前記フラグ設定制御手段は、初期暗号化の実行中を示す初期暗号化実行中フラグを有することを特徴とする請求項１４記載の光加入者線端局装置。

【請求項１７】　前記フラグ設定制御手段は、前記受信装置に対する前記暗号化設定情報の設定更改が失敗と判断した場合は、設定更改失敗フラグをセットすることを特徴とする請求項１４記載の光加入者線端局装置。

【請求項１８】　前記フラグ設定制御手段は、前記受信装置が状態落ちしたと判断した場合は、設定更改未完了フラグをセットすることを特徴とする請求項１４記載の光加入者線端局装置。

【請求項１９】　前記フラグ設定制御手段は、暗号化の更改周期中に暗号化更改中フラグをセットすることを特徴とする請求項１４記載の光加入者線端局装置。

【請求項２０】　前記フラグ設定制御手段は、前記暗号化設定情報の設定更改を行う際には、設定更改要求フラグをセットすることを特徴とする請求項１４記載の光加入者線端局装置。

【請求項２１】　前記フラグ設定制御手段は、１つの前記受信装置につき、１つの前記論理コネクションの更改に対して、前記設定更改要求フラグをセットすることを特徴とする請求項２０記載の光加入者線端局装置。

【請求項２２】　前記フラグ設定制御手段は、前記暗号化設定情報の設定更改実行中には、設定更改実行中フラグをセットすることを特徴とする請求項１４記載の光加入者線端局装置。

【請求項２３】　前記暗号化設定情報を前記受信装置へ再度送信する上書き処理を行う暗号化設定情報上書き手段をさらに有することを特徴とする請求項１４記載の光加入者線端局装置。

【請求項２４】　前記暗号化設定情報上書き手段は、優先度の高い他のメッセージの送信を行う場合は、前記上書き処理を待機させることを特徴とする請求項２３記載の光加入者線端局装置。

【請求項２５】　前記暗号化設定情報上書き手段は、前記暗号化設定情報の設定更改実行中は、前記上書き処理を待機させることを特徴とする請求項２３記載の光加入者線端局装置。

【請求項２６】　前記暗号化設定情報上書き手段は、タイマを有し、前記タイマに設定された周期にしたがって、前記上書き処理を行うことを特徴とする請求項２３記載の光加入者線端局装置。

【請求項２７】　前記タイマの周期は、外部から任意の値に設定されることを特徴とする請求項２６記載の光加入者線端局装置。

【請求項２８】　前記暗号化設定情報送信制御手段は、前記暗号化設定情報を複数回送信する場合に、１回目の前記暗号化設定情報の送信時のみ他メッセージと調停処理を行い、調停後は前記暗号化設定情報を一定間隔毎に自動的に送信することを特徴とする請求項１４記載の光加入者線端局装置。

【請求項２９】　前記暗号鍵の暗号鍵更改タイミング

で、前記暗号化設定情報の更改を開始する暗号化設定情報更改手段をさらに有することを特徴とする請求項１４記載の光加入者線端局装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は光加入者線終端装置及び光加入者線端局装置に関し、特に光加入者系システムに接続して情報ストリームを受信し、暗号鍵を用いて、暗号化された情報部分の復号化を行う光加入者線終端装置、及び光加入者系システムに接続して、暗号鍵を用いて暗号化を行った情報部分を含む情報ストリームを送信する光加入者線端局装置に関する。

【０００２】

【従来の技術】近年、通信サービスの多様化は加速し、ビデオ・オン・デマンド、ＣＡＴＶ、高速コンピュータ通信等の需要が拡大しつつある。このような大容量の通信サービスを低料金で提供するためには、加入者通信網を光化した光加入者系システムが不可欠である。

【０００３】光加入者系システムとしては、１本の光ファイバを複数の加入者で共有するＰＤＳ（Passive Double Star)が提案されている。また、特に欧州を中心にしてＰＤＳ方式を採用したＰＯＮ（Passive Optical Network)システムが注目されており、光ファイバを各家庭まで敷設するＦＴＴＨ（Fiber To The Home)システムの実現へ向けて開発が進んでいる。

【０００４】また、このようなＦＴＴＨシステムの実現のためには、音声や動画などのリアルタイムの通信要求に対して、通信帯域や品質を保証するために、ＡＴＭ（Asynchronous Transfer Mode）を利用したＡＴＭ－ＰＯＮの構築が、ＦＳＡＮ（FullService Access Networks：光通信事業を推進するために設立された国際的な通信業界団体）を中心に進められている。

【０００５】図２５はＡＴＭ－ＰＯＮシステムの構成を示す図である。加入者宅１００ａ～１００ｎ内には、光バースト伝送を行うＯＮＵ（Optical Network Unit：光加入者線終端装置）１０１ａ～１０１ｎが配置され、局２００内にはＯＬＴ（Optical Line Terminal ：光加入者線端局装置）２０１が配置される。

【０００６】ＯＮＵ１０１ａ～１０１ｎには電話機やＣＡＴＶ等が接続され、ＯＬＴ２０１には交換機（ＡＴＭ交換機、ＩＳＤＮ交換機等）２０２が接続する。また、ＯＮＵ１０１ａ～１０１ｎとＯＬＴ２０１は、スターカプラ３００と接続する。

【０００７】局２００から加入者宅１００ａ～１００ｎへの下り情報（下りセル）は、１本の光ファイバから、スターカプラ３００を介して、樹枝状に分岐された光ファイバを通じて送信される。また、加入者宅１００ａ～１００ｎから局２００への上り情報（上りセル）は、樹枝状に分岐された光ファイバから、スターカプラ３００を介して、１本に集約された光ファイバを通じて送信される。

【０００８】このように、ＡＴＭ－ＰＯＮシステムは、スターカプラ３００で局と複数の加入者とを１：ｎで接続して構成する、ＡＴＭを使った光分岐型のアクセスネットワークである。

【０００９】ここで、ＯＬＴ２０１からＯＮＵ１０１ａ～１０１ｎへの下り通信は、放送型であるため、ＩＴＵ－Ｔ勧告Ｇ．９８３では、ＯＮＵ毎の秘匿性を目的として、暗号化（Ｃｈｕｒｎｉｎｇ）方式が規定されている。

【００１０】まず、ＯＬＴ２０１は、下りメッセージにより、ＯＮＵ（例えば、ＯＮＵ１０１ａ）に暗号鍵を要求する。すると、応答したＯＮＵ１０１ａは、暗号鍵を生成し、ＯＬＴ２０１に通知する。

【００１１】ＯＬＴ２０１は、その暗号鍵を使用して、ＯＮＵ１０１ａに対して送信すべき下り情報に対して暗号化を施す。この下り情報の暗号化はＶＰ（Virtual Path：仮想パス）毎に行われる。

【００１２】この場合、ＯＬＴ２０１は、ＯＮＵ１０１ａに対し、ＶＰＩ（Virtual Path Identifier ：仮想パス識別子）を単位として、どのＶＰに対して暗号化を施した（ＯＮ）か否か（ＯＦＦ）を示す設定情報である暗号化設定情報を下りメッセージにより通知する。

【００１３】このように、ＡＴＭ－ＰＯＮシステムの暗号化方式では、暗号鍵はＯＮＵ毎に割り当てられ、下り情報の暗号化のＯＮ／ＯＦＦはＶＰＩ単位で行われる。そして、ＯＬＴ２０１がＯＮＵ１０１ａに下りメッセージを用いて、暗号化設定情報を通知し、ＯＮＵ１０１ａでは自己の暗号鍵を用いて、暗号化されたＶＰの下り情報を復号化する。

【００１４】

【発明が解決しようとする課題】しかし、上記のようなＩＴＵ－Ｔ勧告Ｇ．９８３におけるＡＴＭ－ＰＯＮシステムの暗号化方式では、詳細な処理手順が規定されていない。

【００１５】例えば、ＯＮＵ１０１ａでは、ＯＬＴ２０１からの暗号化設定情報を保持しているが、ＩＴＵ－Ｔ勧告Ｇ．９８３には復号化処理をいつ有効にすべきかが規定されていない。

【００１６】したがって、ＯＬＴ２０１側での暗号化処理、ＯＮＵ１０１ａ側での復号化処理それぞれに時間的に大きなずれがあった場合などでは、暗号化・復号化が正常に行えないといった問題があった。

【００１７】また、暗号化設定情報は、ＯＮＵの電源断時にはリセットされるため、電源復旧後は再度設定を行う必要があり、再立ち上げに時間がかかるなどといった問題もある。

【００１８】このように、従来のＡＴＭ－ＰＯＮシステムの暗号化方式では、十分な技術が未だ確立されておらず、システム構築の実現のために高品質な通信制御を早

急に確立する必要がある。

【００１９】本発明はこのような点に鑑みてなされたものであり、高品質な通信制御を確立し、情報の受信制御及び復号化処理を効率よく行う光加入者線終端装置を提供することを目的とする。

【００２０】また、本発明の他の目的は、高品質な通信制御を確立し、情報の送信制御を効率よく行う光加入者線端局装置を提供することである。

【００２１】

【課題を解決するための手段】本発明では上記課題を解決するために、図１に示すような、光加入者系システムに接続して情報ストリームを受信し、暗号鍵を用いて、暗号化された情報部分の復号化を行う光加入者線終端装置１０において、論理コネクション毎に暗号化を施したか否かを示す設定情報である暗号化設定情報に対し、現在使用中の暗号化設定情報を記憶するアクティブ側の第１の記憶手段Ｍ１１ａと、新しく更改された暗号化設定情報を記憶するバックアップ側の第２の記憶手段Ｍ１１ｂとを含み、第１の記憶手段Ｍ１１ａ及び第２の記憶手段Ｍ１１ｂへの記憶制御を行い、暗号鍵の暗号鍵更改タイミングで、第１の記憶手段Ｍ１１ａと第２の記憶手段Ｍ１１ｂとの切り替え制御を行う暗号化設定情報記憶手段１１と、フレーム構成を持つ情報ストリームを受信し、記憶している暗号化設定情報を、暗号鍵更改タイミング以後の次フレームから有効にして、暗号化設定情報が示す暗号化された情報部分に対する復号化処理を次フレームから行う暗号化情報復号化処理手段１２と、を有することを特徴とする光加入者線終端装置１０が提供される。

【００２２】ここで、第１の記憶手段Ｍ１１ａは、現在使用中の暗号化設定情報を記憶する。第２の記憶手段Ｍ１１ｂは、新しく更改された暗号化設定情報を記憶する。暗号化設定情報記憶手段１１は、第１の記憶手段Ｍ１１ａと第２の記憶手段Ｍ１１ｂを含み、第１の記憶手段Ｍ１１ａ及び第２の記憶手段Ｍ１１ｂへの記憶制御を行い、暗号鍵の暗号鍵更改タイミングで、第１の記憶手段Ｍ１１ａと第２の記憶手段Ｍ１１ｂとの切り替え制御を行う。暗号化情報復号化処理手段１２は、フレーム構成を持つ情報ストリームを受信し、記憶している暗号化設定情報を、暗号鍵更改タイミング以後の次フレームから有効にして、暗号化設定情報が示す暗号化された情報部分に対する復号化処理を次フレームから行う。

【００２３】また、図１５に示すような、光加入者系システムに接続して、暗号鍵を用いて暗号化を行った情報部分を含む情報ストリームを送信する光加入者線端局装置２０において、受信装置へ情報ストリームを送信する際に、フラグの設定制御を行うフラグ設定制御手段２１と、フラグにもとづいて、論理コネクション毎に暗号化を施したか否かを示す設定情報である暗号化設定情報の送信制御を行う暗号化設定情報送信制御手段２２と、を有することを特徴とする光加入者線端局装置２０が提供される。

【００２４】ここで、フラグ設定制御手段２１は、受信装置へ情報ストリームを送信する際に、フラグの設定制御を行う。暗号化設定情報送信制御手段２２は、フラグにもとづいて、論理コネクション毎に暗号化を施したか否かを示す設定情報である暗号化設定情報の送信制御を行う。

【００２５】

【発明の実施の形態】以下、本発明の実施の形態を図面を参照して説明する。図１は本発明の光加入者線終端装置の原理図である。光加入者線終端装置１０は、ＯＮＵに該当し、ＡＴＭ－ＰＯＮ等の光加入者系システムに接続してＯＬＴから送信される情報ストリーム（複数のセルで構成される）を受信する。

【００２６】そして、自己の装置で生成した暗号鍵を用いて、情報ストリーム内の暗号化された情報部分に対して復号化を行う。以降では、光加入者線終端装置１０をＯＮＵ１０と呼ぶ。

【００２７】暗号化設定情報記憶手段１１は、暗号化設定情報を記憶するために、第１の記憶手段Ｍ１１ａと第２の記憶手段Ｍ１１ｂの２面の記憶領域を有している。ここで、暗号化設定情報とは、論理コネクション毎に暗号化を施したか否かを示す設定情報である。具体的には、ＶＰＩを単位として、どのＶＰに対して暗号化を施したか否かを示す設定情報のことをいう。

【００２８】第１の記憶手段Ｍ１１ａは、アクティブ側であり、現在使用中（読み出し中）の暗号化設定情報を記憶している。第２の記憶手段Ｍ１１ｂは、バックアップ側であり、新しく更改された暗号化設定情報を記憶する。

【００２９】そして、暗号化設定情報記憶手段１１は、第１の記憶手段Ｍ１１ａと第２の記憶手段Ｍ１１ｂへの記憶制御（書き込み制御）を行い、暗号鍵の暗号鍵更改タイミング（古い暗号鍵を新しい暗号鍵に更改した時のタイミング）で、第１の記憶手段Ｍ１１ａと第２の記憶手段Ｍ１１ｂとの切り替え制御を行う。詳細は後述する。

【００３０】暗号化情報復号化処理手段１２は、フレーム構成を持つ情報ストリームを受信し、記憶している暗号化設定情報を第１の記憶手段Ｍ１１ａから読み出して、暗号鍵更改タイミング以後の次フレームから、読み出した暗号化設定情報を有効にする。そして、暗号化設定情報が示す暗号化された情報部分に対する復号化処理を次フレームから行う。

【００３１】例えば、情報ストリーム中の１つのフレームの中で、ＶＰＩ＝“００１”（“００１”はヘキサデータ）の情報が暗号化されている旨が暗号化設定情報に記載されているものとする。また、ＶＰＩ＝“００１”に対応するセルがセルＣ１だとする。

【００３２】図に示すように、暗号化設定情報を受信すると、バックアップ側の第２の記憶手段Ｍ１１ｂに記憶する。その後、暗号鍵アップデートメッセージＭ１を受信して、４８×Ｔフレーム経過した後の暗号鍵更改タイミング以後の次フレームからこの暗号化設定情報を有効にする。このようにして復号化処理の有効タイミングを明確に規定したので、暗号化処理、復号化処理の不一致を防止することが可能になる。なお、詳細動作は後述する。

【００３３】外部記憶制御手段１３は、暗号化設定情報を不揮発性メモリ１３ａに記憶させる。復号化マスク手段１４は、暗号化情報の復号化を行える運用状態から、他の状態へ遷移して再度運用状態になった場合に、運用状態になった時から暗号鍵更改タイミングを受信するまでの期間の復号化処理をマスクする。なお、外部記憶制御手段１３及び復号化マスク手段１４の詳細については後述する。

【００３４】次に本発明のＯＮＵ１０の具体的な構成・動作について詳しく説明する。なお、以降では暗号化処理をＣｈｕｒｎ、復号化処理をＤｅｃｈｕｒｎ、暗号化設定情報をＣｈｕｒｎｅｄ－ＶＰ設定情報と呼ぶ。

【００３５】図２は情報ストリームの構成及びＣｈｕｒｎｅｄ－ＶＰ設定情報のフォーマットを示す図である。ＯＬＴから送信される情報ストリームの１つのフレーム（ＰＬＯＡＭフレーム）は、ＯＬＴとＯＮＵ１０間で制御情報を通信するためのＰＬＯＡＭ（Physical Layer Operation And Management ）セルと、実際の通信情報であるユーザセルＣ１～Ｃ２７から構成される。そして、このＰＬＯＡＭフレーム２つ分で、Ｔフレームと呼ぶ（伝送レートが１５０Ｍｂｐｓモードの場合）。

【００３６】また、ＰＬＯＡＭセル及びユーザセル共に、１セルが５３バイトである。Ｃｈｕｒｎｅｄ－ＶＰ設定情報は、ＰＬＯＡＭセルで送信される各種制御情報のうちの１つであり、ＰＬＯＡＭセルの４０バイト～５１バイトまでがＣｈｕｒｎｅｄ－ＶＰ設定情報として定義されている。

【００３７】４０バイト目は、ＰＯＮ－ＩＤであり、ＯＮＵ１０の識別子としてＰＯＮ－ＩＤが記される。４１バイト目は、Ｃｈｕｒｎｅｄ－ＶＰ設定情報であることを知らせる識別子が記される。この識別子は“００００１１１１”（左側がＭＳＢ、右側がＬＳＢである。以降同様）である。

【００３８】４３、４４バイト目は、ＶＰＩを示す情報であり、４３、４４バイト目に記されるＶＰＩ情報をＶＰＩ〔１１：０〕と表す。また、４３バイト目の“ａｂｃｄｅｆｇｈ”をＶＰＩ〔１１：４〕と表し、４４バイト目の“ｉｊｋｌ”をＶＰＩ〔３：０〕と表す。なお、ＡＴＭ－ＰＯＮシステムのＶＰＩの値は４０９６個ある（４０９６ＶＰある）。また、ユーザセルも、どのＶＰから流れてきたものかを示すために、同様なＶＰＩ情報をそれぞれ個別に有している。

【００３９】ここで、〔Ｍ：Ｎ〕は、下位Ｎビットから上位Ｍビットの（Ｍ－Ｎ＋１）ビットのデータであることを意味する。４２バイト目は、４３、４４バイト目に記されたＶＰＩに対して、Ｃｈｕｒｎされているか否かを示す情報が記される。内容は“ｘｘｘｘｘｘｘａ”（ｘ＝未定義）であり、ａ（アクトビット）＝１ならＣｈｕｒｎされており（したがって、ＯＮＵ１０ではＤｅｃｈｕｒｎしなければならない）、ａ＝０ならＣｈｕｒｎされていない。４５～５１バイト目は未定である。

【００４０】次に暗号鍵更改について説明する。本発明のＯＮＵ１０が適用されるＡＴＭ－ＰＯＮシステムでは、ＯＬＴ側に位置する保守端末装置からの要求毎に、暗号鍵（以降、Ｃｈｕｒｎｉｎｇ－Ｋｅｙと呼ぶ）の更改（鍵を新しくすること）を行っている。図３はＣｈｕｒｎｉｎｇ－Ｋｅｙの更改シーケンスを示す図である。

〔Ｓ１〕ＯＬＴは、新しいＣｈｕｒｎｉｎｇ－Ｋｅｙの送信要求として、Ｃｈｕｒｎｉｎｇ－ＫｅｙアップデートメッセージＭ１をＯＮＵ１０に送信する。

〔Ｓ２〕ＯＮＵ１０は、新しいＣｈｕｒｎｉｎｇ－Ｋｅｙを生成して、ＡＣＫメッセージｍ１に乗せてＯＬＴに返送する。

〔Ｓ３〕ＯＬＴは、Ｃｈｕｒｎｉｎｇ－ＫｅｙアップデートメッセージＭ１を送信してから１６×Ｔフレーム経過した後、Ｃｈｕｒｎｉｎｇ－ＫｅｙアップデートメッセージＭ２をＯＮＵ１０に送信する。

〔Ｓ４〕ＯＮＵ１０は、ステップＳ２と同様に、ＡＣＫメッセージｍ２に更改したＣｈｕｒｎｉｎｇ－Ｋｅｙの情報を乗せてＯＬＴに返送する。

〔Ｓ５〕ＯＬＴは、Ｃｈｕｒｎｉｎｇ－ＫｅｙアップデートメッセージＭ２を送信してから１６×Ｔフレーム経過した後、Ｃｈｕｒｎｉｎｇ－ＫｅｙアップデートメッセージＭ３をＯＮＵ１０に送信する。

〔Ｓ６〕ＯＮＵ１０は、ステップＳ２及びステップＳ４と同様に、ＡＣＫメッセージｍ３をＯＬＴに返送する。

〔Ｓ７〕ＯＬＴがＣｈｕｒｎｉｎｇ－ＫｅｙアップデートメッセージＭ１をＯＮＵ１０へ送信してから４８×Ｔフレーム経過した時点（Ｃｈｕｒｎｉｎｇ－Ｋｅｙ更改タイミング）で、新しいＣｈｕｒｎｉｎｇ－Ｋｅｙが使用される。すなわち、ＯＬＴはこの新しいＣｈｕｒｎｉｎｇ－ＫｅｙでＣｈｕｒｎを行い、ＯＮＵ１０は新しいＣｈｕｒｎｉｎｇ－ＫｅｙでＤｅｃｈｕｒｎを行う。なお、１６×Ｔフレームのカウントは、図に示すようにＯＬＴ、ＯＮＵ１０の双方で行う。

【００４１】したがって、ＯＬＴがＣｈｕｒｎｉｎｇ－ＫｅｙアップデートメッセージＭ１をＯＮＵ１０に送信してから、４８×Ｔフレーム経過するまでは、旧タイプのＣｈｕｒｎｉｎｇ－Ｋｅｙを用いて、ＯＬＴとＯＮＵ１０間でＣｈｕｒｎ／Ｄｅｃｈｕｒｎが行われる。

【００４２】次に暗号化設定情報記憶手段１１の２面Ｒ

AM構成及びコピー動作について説明する。図３で説明したように、Ｃｈｕｒｎｉｎｇ－ＫｅｙをＣｈｕｒｎｉｎｇ－Ｋｅｙ更改タイミングで更改した場合には、Ｃｈｕｒｎｅｄ－ＶＰ設定情報もこのタイミングでＯＮＵ１０側で更改しなければならない。したがって、Ｃｈｕｒｎｉｎｇ－Ｋｅｙ更改タイミングとなる以前にＯＬＴから送信された新しいＣｈｕｒｎｅｄ－ＶＰ設定情報を記憶しておく必要がある。

【００４３】図４は２面ＲＡＭを持つＯＮＵ１０のブロック構成を示す図である。Ｃｈｕｒｎｅｄ－ＶＰメッセージフラグ設定手段１１－１とＣｈｕｒｎｅｄ－ＶＰ設定情報書き込み手段１１－２は暗号化設定情報記憶手段１１内に含まれ、復号化処理手段１２は暗号化情報復号化処理手段１２に対応する。

【００４４】Ｃｈｕｒｎｅｄ－ＶＰメッセージフラグ設定手段１１－１は、ＰＬＯＡＭセルのＣｈｕｒｎｅｄ－ＶＰ設定情報を受信した場合に、Ｃｈｕｒｎｅｄ－ＶＰメッセージフラグをセットする。

【００４５】Ｃｈｕｒｎｅｄ－ＶＰ設定情報書き込み手段１１－２は、Ｃｈｕｒｎｅｄ－ＶＰメッセージフラグをライトイネーブルの１つとして用い、ＲＡＭ Ｍ１１ａ、Ｍ１１ｂ（暗号化設定情報記憶手段１１が含む記憶手段に対応する）にＣｈｕｒｎｅｄ－ＶＰ設定情報の書き込みを行う。ＲＡＭ Ｍ１１ａ、Ｍ１１ｂは、２５６アドレスであり、１アドレスが格納するデータ領域は１６ビットある。 また、切り替え制御手段１１－３とコピー制御手段１１－４は暗号化設定情報記憶手段１１内に含まれる。

【００４６】最初、ＲＡＭ Ｍ１１ａを、アクティブ側（ＲＡＭ Ｍ１１ａのアドレスをＶＰＩ〔１１：４〕として、現在Ｃｈｕｒｎｅｄ－ＶＰ設定情報が読み出されているＲＡＭ）とし、ＲＡＭ Ｍ１１ｂをバックアップ側（ＯＬＴから送信された新しいＣｈｕｒｎｅｄ－ＶＰ設定情報を次のＣｈｕｒｎｉｎｇ－Ｋｅｙ更改タイミングまで保持しておくＲＡＭ）とする。

【００４７】切り替え制御手段１１－３は、Ｃｈｕｒｎｉｎｇ－ＫｅｙアップデートメッセージＭ１～Ｍ３を３回受信して、Ｃｈｕｒｎｉｎｇ－ＫｅｙアップデートメッセージＭ１から４８×Ｔフレーム経過した場合には、その時間をＣｈｕｒｎｉｎｇ－Ｋｅｙ更改タイミングとして認識する。

【００４８】そして、Ｃｈｕｒｎｉｎｇ－Ｋｅｙ更改タイミングでＲＡＭ Ｍ１１ａとＲＡＭ Ｍ１１ｂを切り替えて、ＲＡＭ Ｍ１１ｂをアクティブ側、ＲＡＭ Ｍ１１ａをバックアップ側とする。

【００４９】一方、このままでは古いＣｈｕｒｎｅｄ－ＶＰ設定情報を記憶しているＲＡＭＭ１１ａがバックアップ側となってしまう。したがって、コピー制御手段１１－４は、新しくアクティブ側になったＲＡＭ Ｍ１１ｂからデータをＲＡＭ Ｍ１１ａへコピーしていく。

【００５０】なお、ＲＡＭ Ｍ１１ａ及びＲＡＭ Ｍ１１ｂは共に読み出しポートを２つ有している。このため、例えば、アクティブ側のＲＡＭからバックアップ側のＲＡＭへコピーが行われている最中でも、アクティブ側ＲＡＭからＣｈｕｒｎｅｄ－ＶＰ設定情報を読み出すことができる。

【００５１】図５はコピー動作手順を示すフローである。なお、最初はＲＡＭ Ｍ１１ａをアクティブ側、ＲＡＭ Ｍ１１ｂをバックアップ側とし、ＲＡＭ Ｍ１１ａとＲＡＭ Ｍ１１ｂのそれぞれは、図に示すような値（例えば、“０００”＝１とは、ＶＰＩ＝“０００”のａビット情報が１ということ）が格納されているものとする。

〔Ｓ１０〕切り替え制御手段１１－３は、Ｃｈｕｒｎｉｎｇ－Ｋｅｙ更改タイミングでＲＡＭ Ｍ１１ａとＲＡＭ Ｍ１１ｂを切り替える。

〔Ｓ１１〕コピー制御手段１１－４は、切り替え制御手段１１－３から通知されたＣｈｕｒｎｉｎｇ－Ｋｅｙ更改タイミングを受信すると、ＲＡＭ Ｍ１１ｂに対する読み出しアドレスをインクリメントして、ＲＡＭ Ｍ１１ｂからデータを読み出す。

〔Ｓ１２〕コピー制御手段１１－４は、ＲＡＭ Ｍ１１ａに対する書き込みアドレスをインクリメントして、ＲＡＭ Ｍ１１ｂから読み出したデータをＲＡＭ１１ａへ書き込んでいく。

〔Ｓ１３〕コピー制御手段１１－４は、書き込みアドレスが最大になったか否かを判断する。最大でなければステップＳ１１へ戻って、ステップＳ１１、Ｓ１２を繰り返し行い、最大であればコピーを終了する。

【００５２】図６はコピー動作時のタイミングチャートを示す図である。ＫＥＹＴＩＭは、Ｃｈｕｒｎｉｎｇ－Ｋｅｙ更改タイミングパルスである。ＲＡＭ－ＳＴＡＴＥは、２面のＲＡＭがアクティブ側かバックアップ側かを示す信号であり、図では更改前のＲＡＭステートとしてＲＡＭ（Ｂ）がアクティブ側であり、更改後にＲＡＭ（Ａ）がアクティブ側となるものとする。

【００５３】ＣＯＰＹＭＯＤＥは、コピー動作時に“Ｈ”となる信号である。ＣＯＰＹＣＴＲは、ＣＯＰＹＭＯＤＥが“Ｈ”の間、ＲＡＭの２５６アドレス数をカウントするための信号である。実際には、ＸＷＥが図に示すような位相となるので、２５９進カウンタを用いている。

【００５４】ＲＡＭＡ－ＲＡＤは、新しくアクティブ側になったＲＡＭ（Ａ）の読み出しアドレスを示す信号であり、ＣＯＰＹＣＴＲを１段ずらした信号を読み出しアドレスとして使用する。

【００５５】ＲＡＭＡ－ＲＤＴは、ＲＡＭＡ－ＲＡＤのアドレスで読み出された読み出しデータを示す信号であり、アドレス０に対して読み出しデータＡ、アドレス１に対して読み出しデータＢ、……である。ＲＡＭＡ－Ｒ

ADから１段ずれた位置に読み出しデータが出力される。

【００５６】ＲＡＭＢ－ＷＤＴは、バックアップ側となったＲＡＭ（Ｂ）への書き込みデータを示す信号であり、ＲＡＭＡ－ＲＤＴを１段ずらした信号を書き込みデータとして使用する。

【００５７】ＲＡＭＢ－ＷＡＤは、ＲＡＭＢ－ＷＤＴをＲＡＭ（Ｂ）へ書き込むための書き込みアドレスを示す信号である。アドレス０に対して書き込みデータＡ、アドレス１に対して書き込みデータＢ、……をＲＡＭ（Ｂ）へ書き込んでいく（コピーする）。

【００５８】ＸＷＥは、バックアップ側となったＲＡＭ（Ｂ）へ、ＲＡＭ（Ａ）の内容をコピーする場合の書き込みイネーブル信号であり、アクティブ“Ｌ”である。以上説明したように、本発明では、２面あるＲＡＭの切り替えを行った場合に、新しいＣｈｕｒｎｅｄ－ＶＰ設定情報を、切り替え後にバックアップ側となったＲＡＭへコピーする構成にした。

【００５９】これにより、バックアップ側も新しいＣｈｕｒｎｅｄ－ＶＰ設定情報を絶えず持つことができ、ＯＬＴ側とのＣｈｕｒｎｅｄ－ＶＰ設定情報の不一致を防止することが可能になる。

【００６０】次にコピー中にあらたなＣｈｕｒｎｅｄ－ＶＰ設定情報を受信した場合の動作について説明する。Ｃｈｕｒｎｉｎｇ－Ｋｅｙ更改タイミングは、ＰＬＯＡＭ周期を最小単位として、フレーム数を数えているので必ずＰＬＯＡＭセルの位置で上がることになる。

【００６１】この場合、Ｃｈｕｒｎｉｎｇ－Ｋｅｙ更改タイミングの位置のＰＬＯＡＭセルがＣｈｕｒｎｅｄ－ＶＰ設定情報を持つセルの場合、バックアップ側のＲＡＭへは、アクティブ側のＲＡＭのデータのコピーが開始されているため、その情報をバックアップ側のＲＡＭへ即時に書き込むことができない。

【００６２】そこで、コピー中にこのようなＣｈｕｒｎｅｄ－ＶＰ設定情報を受信した場合には、フラグ（上述したＣＯＰＹＭＯＤＥをフラグとして利用）をセットし、コピー終了後にフラグをクリアして、バックアップ側のＲＡＭへ上書きする構成とする。

【００６３】図７はコピー中にＣｈｕｒｎｅｄ－ＶＰ設定情報を受信した際の動作を示すタイミングチャートである。ＣＯＰＹＭＯＤＥは、コピー動作時に“Ｈ”となる信号である。ＣＨＵＲＮＥＤ－ＴＲは、Ｃｈｕｒｎｅｄ－ＶＰ設定情報を受信したこと示すトリガ信号であり、受信時に“Ｈ”となる。

【００６４】ＣＨＵＲＮＥＤ－ＬＴは、ＣＯＰＹＭＯＤＥが“Ｈ”で、ＣＨＵＲＮＥＤ－ＴＲが“Ｈ”になった場合にＣＨＵＲＮＥＤ－ＴＲをラッチした信号である。ＣＶＰ－ＣＴＲは、ＣＨＵＲＮＥＤ－ＬＴの立ち下がりでロードされて、バックアップ側のＲＡＭへ書き込むための書き込みアドレスを示す信号である。

【００６５】以上説明したように、コピー中に受信したＣｈｕｒｎｅｄ－ＶＰ設定情報に対しては、コピー終了後に書き込む構成とした。このように、コピーを優先して、その後に上書きすることにより、ＲＡＭへのコピー動作時のコピーエラーを防止することが可能になる。

【００６６】次にＣｈｕｒｎｅｄ－ＶＰ設定情報を受信した際の応答信号の返送制御について説明する。ＩＴＵ－Ｔ勧告Ｇ．９８３では、ＯＮＵ１０がＣｈｕｒｎｅｄ－ＶＰ設定情報を受信した場合、受信したことをＯＬＴへ通知するための応答信号を返送する旨が規定されているが、返送条件については規定されていない。

【００６７】したがって、本発明の暗号化設定情報記憶手段１１は、Ｃｈｕｒｎｅｄ－ＶＰ設定情報を受信してＲＡＭへ書き込んだ際に、再度読み出してベリファイチェック（書き込んだ値と読み出した値とを比較する）を行う。そして、正常に書き込めた場合にのみ、ＯＮＵ１０はＯＬＴへ応答信号を返送する。

【００６８】図８は応答信号の返送制御手順を示すフローチャートである。ＲＡＭ（Ａ）をアクティブ側、ＲＡＭ（Ｂ）をバックアップ側とし、コピー動作は終了しているものとする。

【００６９】したがって、Ｃｈｕｒｎｅｄ－ＶＰ設定情報を受信した際には、ＲＡＭ（Ｂ）へ書き込み、再度ＲＡＭ（Ｂ）から読み出してベリファイチェックを行った後に応答信号の返送制御を行う。

〔Ｓ２０〕Ｃｈｕｒｎｅｄ－ＶＰ設定情報を受信する。

〔Ｓ２１〕Ｃｈｕｒｎｅｄ－ＶＰ設定情報が示すアドレスのデータをＲＡＭ（Ｂ）から読み出す。すなわち、ＶＰＩ〔１１：４〕のアドレスに対応するデータのＶＰＩ〔３：０〕の位置にあるデータ（ａビット情報）をＲＡＭ（Ｂ）から読み出す。

〔Ｓ２２〕ＲＡＭ（Ｂ）から読み出したデータのパリティチェック（ＬＳＩ間同士のデータ伝送などでは、データ送受信の信頼性確保のため、誤り訂正を行う必要があり、誤り訂正符号をデータに付加して送受信を行っている）を行う。正常の場合はステップＳ２３へ行く。パリティエラーの場合はステップＳ２９へ行く。

〔Ｓ２３〕ＲＡＭ（Ｂ）から読み出したデータと、受信したＣｈｕｒｎｅｄ－ＶＰ設定情報のａビット情報とを比較する。値が異なる場合はステップＳ２４へ行き、値が同じ場合はステップＳ２５へ行く。

〔Ｓ２４〕ステップＳ２１と同じアドレスへ、更改されたａビット情報を書き込む。

〔Ｓ２５〕ステップＳ２１と同じアドレスからデータを再び読み出す。

〔Ｓ２６〕ＲＡＭ（Ｂ）から読み出したデータのパリティチェックを行う。正常ならばステップＳ２７へ行く。パリティエラーの場合はステップＳ２９へ行く。

〔Ｓ２７〕ＲＡＭ（Ｂ）から読み出したデータと、受信したＣｈｕｒｎｅｄ－ＶＰ設定情報のａビット情報とを

比較する。値が同じ場合はステップＳ２８へ行き、値が異なる場合はステップＳ２９へ行く。

〔Ｓ２８〕ＲＡＭ（Ｂ）へ正常に書き込めたので、Ｃｈｕｒｎｅｄ－ＶＰ設定情報を受信したことを通知するための応答信号をＯＬＴへ返送する。

〔Ｓ２９〕ＯＮＵ１０の全体制御を行っている全体制御部へエラー通知を送信する。

【００７０】以上説明したように、本発明の暗号化設定情報記憶手段１１は、Ｃｈｕｒｎｅｄ－ＶＰ設定情報を受信し、ＲＡＭへ書き込んだ際に正常に書き込めた否かを検証する。そして、ＯＮＵ１０は、正常に書き込めた場合にのみ応答信号を返送する構成とした。これにより、ＯＬＴ側とのＣｈｕｒｎｅｄ－ＶＰ設定情報の設定不一致を防止することが可能になる。

【００７１】次に外部記憶制御手段１３について説明する。本発明のＯＮＵ１０ではバックアップ電源を有しており、外部記憶制御手段１３は、電源断時にはバックアップ電源を利用して、Ｃｈｕｒｎｅｄ－ＶＰ設定情報を不揮発性メモリ（フラッシュメモリなど）１３ａに記憶させる。

【００７２】これにより、電源断になっても不揮発性メモリ１３ａにＣｈｕｒｎｅｄ－ＶＰ設定情報を保持することができるので、電源復旧後に再度Ｃｈｕｒｎｅｄ－ＶＰ設定情報をＯＬＴから送信要求しなくてもよい。

【００７３】また、外部記憶制御手段１３は、一旦、不揮発性メモリ１３ａにＣｈｕｒｎｅｄ－ＶＰ設定情報を格納した後は、あらたに受信したＣｈｕｒｎｅｄ－ＶＰ設定情報と、バックアップ側のＲＡＭに格納されているＣｈｕｒｎｅｄ－ＶＰ設定情報とを比較し、異なるＣｈｕｒｎｅｄ－ＶＰ設定情報のみを不揮発性メモリ１３ａに記憶させる。

【００７４】具体的には、図８のステップＳ２４で、更改されたａビット情報を書き込んだ際に、ａビット情報が更改されていることを示す更改フラグを暗号化設定情報記憶手段１１がセットする。

【００７５】外部記憶制御手段１３は、この更改フラグが立っている場合に、バックアップ側のＲＡＭから、対応するアドレスのデータを読み出し、不揮発性メモリ１３ａへ記憶させる。このように、更改されたＣｈｕｒｎｅｄ－ＶＰ設定情報だけを記憶していくので効率よく不揮発性メモリ１３ａに記憶させることができる。

【００７６】一方、不揮発性メモリ１３ａには書き込み回数が制限されているものが多いため、さらに書き込み回数を削減する工夫が必要である。したがって、外部記憶制御手段１３では、電源復旧時にはＣｈｕｒｎｅｄ－ＶＰ設定情報を例えばＳＲＡＭ（Static-RAM）等のメモリに一旦記憶させ、電源断時にＳＲＡＭから不揮発性メモリ１３ａへ、一括してＣｈｕｒｎｅｄ－ＶＰ設定情報記憶させてもよい。これにより、不揮発性メモリ１３ａへのアクセス回数を削減することが可能になる。

【００７７】また、一旦不揮発性メモリ１３ａからＳＲＡＭへ一括書き込みを行った初期動作以降は、更改フラグが立っているＣｈｕｒｎｅｄ－ＶＰ設定情報のみをＳＲＡＭへ書き込む。そして、電源断時にはＳＲＡＭから不揮発性メモリ１３ａへ、更改されたＣｈｕｒｎｅｄ－ＶＰ設定情報のみを記憶させてもよい。

【００７８】図９は更改されたＣｈｕｒｎｅｄ－ＶＰ設定情報をＳＲＡＭから不揮発性メモリ１３ａへ記憶させる場合の処理手順を示すフローチャートである。

〔Ｓ３０〕暗号化設定情報記憶手段１１は、Ｃｈｕｒｎｅｄ－ＶＰ設定情報が更改されている場合は、更改フラグを立てる。

〔Ｓ３１〕外部記憶制御手段１３は、バックアップ側のＲＡＭから、更改フラグにもとづいて対応するＣｈｕｒｎｅｄ－ＶＰ設定情報を読み出す。

〔Ｓ３２〕外部記憶制御手段１３は、更改されたＣｈｕｒｎｅｄ－ＶＰ設定情報をＳＲＡＭへ書き込む。

〔Ｓ３３〕外部記憶制御手段１３は、ＯＮＵ１０の電源断時に、ＳＲＡＭが格納している情報を不揮発性メモリ１３ａへ書き込む。

【００７９】電源断時には、更改されたＣｈｕｒｎｅｄ－ＶＰ設定情報のみをＳＲＡＭから不揮発性メモリ１３ａへ記憶させてもよい。これにより、不揮発性メモリ１３ａへのアクセス回数をさらに削減することが可能になる。

【００８０】次に電源復旧時のＯＮＵ１０の動作について説明する。ＩＴＵ－Ｔ勧告Ｇ．９８３では、ＯＮＵの動作状態としてＯ１状態～Ｏ１０状態を定めており、特にＯＮＵの電源復旧後の状態は、Ｏ１状態またはＯ９状態であることが規定されている。

【００８１】Ｏ１状態とは、ＯＮＵの電源復旧後の初期状態のことである。Ｏ９状態とは、緊急停止状態であり、この状態になると、ＯＮＵはネットワークから切り離されて、通信ができなくなる。

【００８２】また、本発明では、ＯＮＵ１０の電源復旧後の動作状態として、Ｏ１状態へ遷移させるべきか、またはＯ９状態へ遷移させるべきかを判断するための立ち上げ準備状態（以降、Ｏ０状態と呼ぶ）をあらたに設けることにした。

【００８３】本発明の暗号化設定情報記憶手段１１では、このＯ０状態を利用して、電源復旧時のＯ０状態の期間のみに、不揮発性メモリ１３ａからＣｈｕｒｎｅｄ－ＶＰ設定情報を受け付けることにする。

【００８４】これにより、ＯＮＵ１０の運用状態（以降、Ｏ８状態と呼ぶ）中に、誤ってＲＡＭに対する外部からの書き込みがあった場合でもその情報を有効としないので、ＯＬＴ側とのＣｈｕｒｎｅｄ－ＶＰ設定情報の不一致を防止することが可能になる。

【００８５】一方、暗号化設定情報記憶手段１１は、Ｏ０状態の時に、不揮発性メモリ１３ａから読み出された

Ｃｈｕｒｎｅｄ－ＶＰ設定情報と、あらたに送信された暗号化設定情報とのいずれを有効にすべきか判断して選択することができる。

【００８６】すなわち、ＯＮＵ１０は、Ｏ０状態時に不揮発性メモリ１３ａから再ロードしたＣｈｕｒｎｅｄ－ＶＰ設定情報を有効にするかどうかは未定とする。なぜなら、ＯＬＴから送信される、あらたなＣｈｕｒｎｅｄ－ＶＰ設定情報をＯＮＵ１０へ設定したい（有効としたい）場合があるからである。そこで、２面あるＲＡＭのうち、一方を不揮発性メモリ１３ａからロードした値を持っておくＲＡＭ、他方をＮｏｔＣｈｕｒｎにするためにイニシャライズ（以降、ＮｏｔＣｈｕｒｎ設定と呼ぶ）をかけたＲＡＭをＯ０状態時に設定しておく。

【００８７】そして、不揮発性メモリ１３ａからロードした値を有効にしたい場合は、外部フラグをセットし、そのロードした値をＲＡＭに保持させ、その後、受信したＣｈｕｒｎｅｄ－ＶＰ設定情報をこのＲＡＭに上書きしていく。

【００８８】また、外部フラグがセットされていない場合は、ＯＬＴからのＣｈｕｒｎｅｄ－ＶＰ設定情報を、ＮｏｔＣｈｕｒｎ設定されたＲＡＭへ書き込んでいく。それぞれの場合ともＣｈｕｒｎｉｎｇ－Ｋｅｙ更改タイミングで、コピー動作が開始される。

【００８９】図１０は暗号化設定情報記憶手段１１の電源復旧時の動作状態を示すフローチャートである。ＲＡＭ（Ａ）をＮｏｔＣｈｕｒｎ設定されたＲＡＭとし、ＲＡＭ（Ｂ）を不揮発性メモリ１３ａからロードされたＣｈｕｒｎｅｄ－ＶＰ設定情報を保持するロード値設定ＲＡＭとする。なお、期間Ｂではユーザセルは Ｎｏｔ Ｄｅｃｈｕｒｎである。

〔Ｓ４０〕外部フラグがセットされているか否かを判断する。セットしていればステップＳ４１へ、セットしていなければステップＳ４５へ行く。

〔Ｓ４１〕ＲＡＭ（Ａ）をアクティブ側、ＲＡＭ（Ｂ）をバックアップ側と設定する。

〔Ｓ４２〕Ｃｈｕｒｎｅｄ－ＶＰ設定情報を受信した場合は、ＲＡＭ（Ｂ）へ上書きする。

〔Ｓ４３〕Ｃｈｕｒｎｉｎｇ－Ｋｅｙ更改タイミングで、ＲＡＭ（Ａ）をバックアップ側、ＲＡＭ（Ｂ）をアクティブ側に設定する。

〔Ｓ４４〕ＲＡＭ（Ｂ）の内容をＲＡＭ（Ａ）へコピーする。

〔Ｓ４５〕Ｃｈｕｒｎｅｄ－ＶＰ設定情報を受信した場合はステップＳ４６へ、受信しない場合はステップＳ４０へ戻る。

〔Ｓ４６〕ＲＡＭ（Ａ）をバックアップ側、ＲＡＭ（Ｂ）をアクティブ側と設定する。

〔Ｓ４７〕Ｃｈｕｒｎｅｄ－ＶＰ設定情報を受信した場合は、ＲＡＭ（Ａ）へ上書きする。

〔Ｓ４８〕Ｃｈｕｒｎｉｎｇ－Ｋｅｙ更改タイミングで、ＲＡＭ（Ａ）をアクティブ側、ＲＡＭ（Ｂ）をバックアップ側に設定する。

〔Ｓ４９〕ＲＡＭ（Ａ）の内容をＲＡＭ（Ｂ）へコピーする。

【００９０】次に復号化マスク手段１４について説明する。ＯＮＵ１０ではＯ８状態になってからＤｅｃｈｕｒｎを行う。また、Ｏ８状態から他の状態に遷移して、再度Ｏ８状態になった時には、ＯＬＴとＯＮＵ１０のＣｈｕｒｎｉｎｇ－Ｋｅｙが一致していないと、ユーザセルに対して誤ったＤｅｃｈｕｒｎを行ってしまう可能性がある。したがって、その間は復号化処理をマスクする必要がある。図１１は復号化マスク処理を示す図である。

〔Ｓ５０〕ＯＮＵ１０がＯ８状態から、その他の状態へ遷移する。

〔Ｓ５１〕復号化マスク手段１４は、Ｏ８状態からその他の状態へ遷移した時にマスクフラグをセットする。

〔Ｓ５２〕復号化マスク手段１４は、Ｄｅｃｈｕｒｎのマスクを開始する（ＮｏｔＤｅｃｈｕｒｎ）。

〔Ｓ５３〕その他の状態からＯ８状態へ遷移する。

〔Ｓ５４〕復号化マスク手段１４は、Ｏ８状態になってから、最初のＣｈｕｒｎｉｎｇ－Ｋｅｙ更改タイミングを受信した場合に、マスクフラグをクリアして、Ｄｅｃｈｕｒｎのマスク解除を行う。

〔Ｓ５５〕新しいＣｈｕｒｎｉｎｇ－Ｋｅｙと新しいＣｈｕｒｎｅｄ－ＶＰ設定情報にもとづいて、Ｄｅｃｈｕｒｎを行っていく。

【００９１】このように、復号化マスク手段１４は、Ｏ８状態に遷移してからＣｈｕｒｎｉｎｇ－Ｋｅｙ更改タイミングとなるまでの期間は、復号化処理をマスクしてＤｅｃｈｕｒｎをかけず、ユーザセルはすべてＮｏｔＣｈｕｒｎとする。

【００９２】これにより、ＯＬＴとＯＮＵ１０のＣｈｕｒｎｉｎｇ－Ｋｅｙの一致を確認して初めてＤｅｃｈｕｒｎを行うことができるので、セルの誤ったＤｅｃｈｕｒｎを防止することが可能になる。

【００９３】次に本発明の変形例について説明する。図１２はＯＮＵ１０の変形例を示す図である。なお、外部記憶制御手段１３は、上述したので説明は省略する。暗号化設定情報記憶手段１１ａは、Ｃｈｕｒｎｅｄ－ＶＰ設定情報を記憶する記憶領域を１つだけ有している。

【００９４】暗号化情報復号化処理手段１２ａは、フレーム構成を持つ情報ストリームを受信し、暗号化設定情報記憶手段１１ａで記憶しているＣｈｕｒｎｅｄ－ＶＰ設定情報を次フレームから有効にする。そして、Ｃｈｕｒｎｅｄ－ＶＰ設定情報が示す暗号化された情報部分に対する復号化処理を次フレームから行う。

【００９５】例えば、情報ストリーム中の１つのフレームの中で、ＶＰＩ＝“００１”（“００１”はヘキサデータ）の情報が暗号化されている旨がＣｈｕｒｎｅｄ－ＶＰ設定情報に記載されているものとする。また、ＶＰ

Ｉ＝“００１”に対応するセルがセルＣ１だとする。

【００９６】このような暗号化設定情報を１フレーム目にＯＮＵ１０ａが受信した場合には、Ｃｈｕｒｎｅｄ－ＶＰ設定情報を暗号化設定情報記憶手段１１ａから読み出した後、次の２フレーム目からこのＣｈｕｒｎｅｄ－ＶＰ設定情報を有効にする。すなわち、２フレーム目からセルＣ１の復号化処理を行っていく。

【００９７】このように、変形例であるＯＮＵ１０ａでは記憶領域が１つだけでよく、また、Ｃｈｕｒｎｉｎｇ－Ｋｅｙの更改時期と独立して、Ｃｈｕｒｎｅｄ－ＶＰ設定情報の有効タイミングを規定した。これにより、効率のよい復号化処理を行うことが可能になる。

【００９８】図１３は次フレームでＤｅｃｈｕｒｎを実現するためのブロック構成を示す図である。なお、Ｃｈｕｒｎｅｄ－ＶＰメッセージフラグ設定手段１１－１とＣｈｕｒｎｅｄ－ＶＰ設定情報書き込み手段１１－２は暗号化設定情報記憶手段１１内に含まれ、復号化処理手段１２は暗号化情報復号化処理手段１２に対応する。

【００９９】Ｃｈｕｒｎｅｄ－ＶＰメッセージフラグ設定手段１１－１は、ＰＬＯＡＭセルのＣｈｕｒｎｅｄ－ＶＰ設定情報を受信した場合に、Ｃｈｕｒｎｅｄ－ＶＰメッセージフラグをセットする。

【０１００】Ｃｈｕｒｎｅｄ－ＶＰ設定情報書き込み手段１１－２は、Ｃｈｕｒｎｅｄ－ＶＰメッセージフラグをライトイネーブルの１つとして用い、ＲＡＭ１１ａ（暗号化設定情報記憶手段１１が含む記憶手段に対応する）にＣｈｕｒｎｅｄ－ＶＰ設定情報の書き込みを行う。ＲＡＭ１１ａは、２５６アドレスであり、１アドレスが格納するデータ領域は１６ビットある。

【０１０１】書き込み処理としては、ＶＰＩ〔１１：０〕のうち、ＶＰＩ〔１１：４〕の８ビットをＲＡＭ１１ａへの書き込みアドレスとし、ａビット情報をＲＡＭ１１ａへの書き込みデータとする。

【０１０２】ここで、ＶＰＩ〔１１：４〕をＲＡＭ１１ａのアドレスとした場合に、この１つのアドレスに１６ビットの格納領域があるため、１アドレスにＶＰＩ〔３：０〕（４ビット）の１６通りのＶＰＩ値を割り当てることができる。

【０１０３】すなわち、ＲＡＭの１つのアドレスに対して、１６通りのＶＰＩを設定でき、この１６通りのＶＰＩに対応するａビット情報を、ＲＡＭ１１ａの格納領域である１６ビットの各ビットに対してデータとして書き込んでいく。したがって、ＲＡＭ１１ａは、４０９６個のａビット情報の記憶領域を有することになる。

【０１０４】復号化処理手段１２は、情報ストリームを受信し、ユーザセルに記載されているＶＰＩ〔１１：０〕を抽出する。そして、抽出したＶＰＩ〔１１：０〕のＶＰＩ〔１１：４〕をＲＡＭ１１ａへの読み出しアドレスとし、ＶＰＩ〔３：０〕に対応する位置にあるビットのａビット情報を読み出しデータとする。ａビット情報＝１ならば、そのセルを暗号鍵を用いてＤｅｃｈｕｒｎし、ａビット情報＝０ならば、ＮｏｔＤｅｃｈｕｒｎ（復号化を行わずスルー）とする。

【０１０５】図１４は次フレームからＤｅｃｈｕｒｎを行う際のタイミングチャートを示す図である。情報ストリームのＰＬＯＡＭセルａのＣｈｕｒｎｅｄ－ＶＰ設定情報に、ＶＰＩ〔１１：０〕＝“００１”（“００１”はヘキサデータ）の情報がＣｈｕｒｎされている（ａビット情報＝１）旨が記載されているものとする。

【０１０６】Ｃｈｕｒｎｅｄ－ＶＰメッセージフラグ設定手段１１－１は、ＰＬＯＡＭセルａを受信して、４１バイト目のＣｈｕｒｎｅｄ－ＶＰ設定情報のＩＤを認識すると、Ｃｈｕｒｎｅｄ－ＶＰメッセージフラグを図に示す位相で出力する。

【０１０７】また、Ｃｈｕｒｎｅｄ－ＶＰ設定情報書き込み手段１１－２は、ＶＰＩ〔１１：０〕＝“００１”及びａビット情報（＝１）を次フレームのユーザセルＣ１の区間まで内部でラッチする。

【０１０８】そして、Ｃｈｕｒｎｅｄ－ＶＰメッセージフラグとＰＬＯＡＭパルス（ＰＬＯＡＭセルの位置を示すパルス）との論理をとった信号をライトイネーブルとして、図に示すセルＦＰ（セルの位置を示すパルス）の位置で、ＶＰＩ〔１１：４〕＝“００”をＲＡＭ１１ａの書き込みアドレス、１６ビットのＶＰＩ〔３：０〕＝“１”の位置にａビット情報を書き込みデータとしてＲＡＭ１１ａに書き込む。

【０１０９】このように、ＰＬＯＡＭセルａを受信した後、次フレームのＰＬＯＡＭセルｂの先頭位置でＰＬＯＡＭセルａにあったＣｈｕｒｎｅｄ－ＶＰ設定情報をＲＡＭ１１ａに書き込み、その後、復号化処理手段１２で読み出して、図に示す位置Ａ（次フレームのユーザセルＣ１の先頭）からＶＰＩ〔１１：０〕＝“００１”に対応するセルのＤｅｃｈｕｒｎを行っていく。ここではＶＰＩ〔１１：０〕＝“００１”はセルＣ１としたので、位置Ａからセル Ｃ１のＤｅｃｈｕｒｎが行われる。

【０１１０】一方、情報ストリームのＰＬＯＡＭセルｂのＣｈｕｒｎｅｄ－ＶＰ設定情報に、ＶＰＩ〔１１：０〕＝“０１０”とあり、Ｃｈｕｒｎされていない（ａビット情報＝０）旨が記載されている場合には、図に示すようなタイミングでＶＰＩ〔１１：０〕＝“０１０”はＮｏｔＤｅｃｈｕｒｎとなる。

【０１１１】このように、本発明のＯＮＵ１０では、ＯＬＴがＰＬＯＡＭセルに設定したＣｈｕｒｎｅｄ－ＶＰ設定情報を、次フレームにあるＰＬＯＡＭセル以降から有効にするような構成とした。

【０１１２】これにより、次フレームのユーザセルから即時にＤｅｃｈｕｒｎ処理を行うことができるので、暗号化処理と復号化処理の不一致防止、さらにデータ疎通時間を短縮させることが可能になる。

【０１１３】次に本発明の光加入者線端局装置について

説明する。図１５は本発明の光加入者線端局装置の原理図である。光加入者線端局装置２０は、ＡＴＭ－ＰＯＮのような光加入者系システムに接続し、暗号鍵を用いて、暗号化を行った情報部分を含む情報ストリームをＯＮＵ３０ａ～３０ｎ（総称してＯＮＵ３０）へ送信する。以降では、光加入者線端局装置２０をＯＬＴ２０と呼ぶ。

【０１１４】ＯＬＴ２０は、フラグ設定制御手段２１と、暗号化設定情報送信制御手段２２と、暗号化設定情報上書き手段２３と、暗号化設定情報更改手段２４から構成される。

【０１１５】フラグ設定制御手段２１は、情報ストリームの送信時にＯＮＵ３０の装置状態等にもとづいて、フラグを設定する。暗号化設定情報送信制御手段２２は、設定されたフラグにもとづいて、論理コネクション毎に暗号化を施したか否かを示す設定情報である暗号化設定情報（Ｃｈｕｒｎｅｄ－ＶＰ設定情報）の送信制御を行う。

【０１１６】暗号化設定情報上書き手段２３は、Ｃｈｕｒｎｅｄ－ＶＰ設定情報をＯＮＵ３０へ再度送信する上書き処理を行う。暗号化設定情報更改手段２４は、Ｃｈｕｒｎｅｄ－ＶＰ設定情報の更改タイミングを暗号化の更改周期終了時に一致させる。

【０１１７】次にフラグ設定制御手段２１の初期暗号化（以下、初期Ｃｈｕｒｎ）フラグについて説明する。ＯＬＴ２０は、停止状態から運用状態（Ｏ８状態）へ遷移したＯＮＵ３０ａに対し、Ｃｈｕｒｎｅｄ－ＶＰ設定情報を送信する。ＯＮＵ３０が停止状態からＯ８状態へ遷移した時に、Ｃｈｕｒｎｅｄ－ＶＰ設定情報を送信することを初期Ｃｈｕｒｎと呼ぶ。

【０１１８】フラグ設定制御手段２１では、初期Ｃｈｕｒｎフラグを設けて、この初期Ｃｈｕｒｎを実行する。初期Ｃｈｕｒｎフラグの設定制御としては、ＯＮＵ３０が停止状態で初期Ｃｈｕｒｎフラグをクリアし（０とし）、初期Ｃｈｕｒｎ完了で初期Ｃｈｕｒｎフラグをセットする（１とする）。

【０１１９】暗号化設定情報送信制御手段２２は、ＯＮＵ３０がＯ８状態へ遷移した時に、この初期Ｃｈｕｒｎフラグをチェックし、初期Ｃｈｕｒｎフラグがセットされていなければ、初期Ｃｈｕｒｎを実行する。

【０１２０】図１６は初期Ｃｈｕｒｎフラグを用いた初期Ｃｈｕｒｎ処理手順を示すフローチャートである。なお、ＯＮＵには固有の番号ｎが与えられており、ＯＮＵの装置状態と後述する各種のフラグはｎで管理される。

〔Ｓ６０〕フラグ設定制御手段２１は、ＯＮＵ（ｎ）が停止状態の場合に初期Ｃｈｕｒｎフラグ（ｎ）を０とする。

〔Ｓ６１〕ＯＮＵ（ｎ）が停止状態からＯ８状態へ遷移する。

〔Ｓ６２〕フラグ設定制御手段２１は、Ｏ８状態に遷移したＯＮＵ（ｎ）が、初期Ｃｈｕｒｎフラグ（ｎ）が０であるか否かを判断する。０ならばステップＳ６３へ行き、１ならば初期Ｃｈｕｒｎ完了とみなして終了する。

〔Ｓ６３〕暗号化設定情報送信制御手段２２は、初期Ｃｈｕｒｎを実行する。ここで、初期Ｃｈｕｒｎでは、ＯＮＵ（ｎ）に対して、４０９６ＶＰ分のＣｈｕｒｎｅｄ－ＶＰ設定情報を送信する。ＯＮＵ（ｎ）に対して、４０９６ＶＰ分のＣｈｕｒｎｅｄ－ＶＰ設定情報の送信が完了し、ＯＮＵ（ｎ）からメッセージ正常受信を通知するＡｃｋを、４０９６ＶＰ分受信すると初期Ｃｈｕｒｎは完了となり、初期Ｃｈｕｒｎフラグ（ｎ）を１とする。

【０１２１】以上説明したように、初期Ｃｈｕｒｎフラグを設けて、初期Ｃｈｕｒｎフラグを ＯＮＵ３０が停止状態でクリア、初期Ｃｈｕｒｎの完了時にセットすることにした。

【０１２２】これにより、ＯＮＵ３０が停止状態からＯ８状態へ遷移した時だけに初期Ｃｈｕｒｎを実行することができ、他の状態から遷移した時には初期Ｃｈｕｒｎを実行せず、無駄な処理を省くことが可能になる。

【０１２３】次にフラグ設定制御手段２１の初期Ｃｈｕｒｎ実行中フラグについて説明する。初期Ｃｈｕｒｎを行う場合には、初期Ｃｈｕｒｎ実行中フラグを設け、初期Ｃｈｕｒｎの実行中はこの初期Ｃｈｕｒｎ実行中フラグをセットする。そして、初期Ｃｈｕｒｎ実行中フラグがセットされている場合は、次の初期Ｃｈｕｒｎ要求を受け付けないことにする。

【０１２４】すなわち、複数のＯＮＵが連続して停止状態からＯ８状態へ遷移した場合などに対し、最初に停止状態からＯ８状態へ遷移したＯＮＵに対して初期Ｃｈｕｒｎを開始し、その時に初期Ｃｈｕｒｎ実行中フラグをセットして、その他のＯＮＵは待機させる。

【０１２５】そして、実行中のＯＮＵの初期Ｃｈｕｒｎが完了すれば、待機しているＯＮＵの初期Ｃｈｕｒｎを開始していく。図１７は初期Ｃｈｕｒｎ実行中フラグを用いた初期Ｃｈｕｒｎ処理手順を示すフローチャートである。

〔Ｓ７０〕フラグ設定制御手段２１は、初期Ｃｈｕｒｎフラグ（ｎ）が０であることを確認する。

〔Ｓ７１〕フラグ設定制御手段２１は、初期Ｃｈｕｒｎ実行中フラグが０であるか否かを判断する。初期Ｃｈｕｒｎ実行中フラグが０であればステップＳ７２へ、１であればステップＳ７４へ行く。

〔Ｓ７２〕フラグ設定制御手段２１は、他のＯＮＵが初期Ｃｈｕｒｎ実行中ではないため、初期Ｃｈｕｒｎ実行中フラグを１とする。

〔Ｓ７３〕暗号化設定情報送信制御手段２２は、該当するＯＮＵ（ｎ）に対して初期Ｃｈｕｒｎを行う。

〔Ｓ７４〕暗号化設定情報送信制御手段２２は、初期Ｃｈｕｒｎ実行中フラグが０になるまで（先行する初期Ｃ

ｈｕｒｎが終了するまで）、初期Ｃｈｕｒｎを待機する。

【０１２６】以上説明したように、初期Ｃｈｕｒｎ実行中フラグが０である場合にのみ、対応するＯＮＵに対して初期Ｃｈｕｒｎを行い、先行する初期Ｃｈｕｒｎが終了した場合に、次のＯＮＵに対して初期Ｃｈｕｒｎを行う構成とした。

【０１２７】これにより、複数のＯＮＵから連続で初期Ｃｈｕｒｎ要求が発生しても、初期ＣｈｕｒｎをＯＮＵ単位のシリアル処理として行うことができるので、複雑な輻輳処理をすることなく、効率よく初期Ｃｈｕｒｎを行うことが可能になる。

【０１２８】次にフラグ設定制御手段２１の設定更改失敗フラグについて説明する。初期Ｃｈｕｒｎが完了したＯＮＵの運用中に、ＯＬＴ２０がＣｈｕｒｎｅｄ－ＶＰ設定情報の設定更改（設定変更）や上書き処理などを行った時に、ＯＮＵ３０へのＣｈｕｒｎｅｄ－ＶＰ設定情報の設定が失敗したとする。

【０１２９】このような、Ｃｈｕｒｎｅｄ－ＶＰ設定情報の設定更改失敗（ＬＯＡｉ（Ｃｈｕｒｎ））が原因で状態落ち（停止状態へ遷移すること）が発生した場合は、再度、Ｏ８状態へ遷移した時に初期Ｃｈｕｒｎを実行する必要がある。

【０１３０】そこで、フラグ設定制御手段２１では、ＯＮＵ３０の運用中にＣｈｕｒｎｅｄ－ＶＰ設定情報の設定失敗の有無を示す設定更改失敗フラグを設ける。暗号化設定情報送信制御手段２２は、設定更改失敗フラグがセットされている場合には、Ｃｈｕｒｎｅｄ－ＶＰ設定情報の設定更改に失敗したものとみなして、該当するＯＮＵ３０に対して初期Ｃｈｕｒｎを実行する。

【０１３１】なお、以降の説明では、初期Ｃｈｕｒｎが完了した運用中のＯＮＵに対して、Ｃｈｕｒｎｅｄ－ＶＰ設定情報の更改を行う場合の処理を、設定更改Ｃｈｕｒｎと呼ぶ。

【０１３２】図１８は設定更改失敗フラグを用いた初期Ｃｈｕｒｎ処理手順を示すフローチャートである。

〔Ｓ８０〕フラグ設定制御手段２１は、Ｃｈｕｒｎｅｄ－ＶＰ設定情報を送信した後、例えば、３００ｍｓ以内にＯＮＵ（ｎ）からメッセージ正常受信を示すＡｃｋを受信しない場合、設定失敗とみなして、設定更改失敗フラグ（ｎ）を１にする。

〔Ｓ８１〕暗号化設定情報送信制御手段２２は、ＯＮＵ（ｎ）に対する各種メッセージの送信を中断する。ＯＮＵ（ｎ）は停止状態となる。

〔Ｓ８２〕暗号化設定情報送信制御手段２２は、設定更改失敗フラグ（ｎ）が１となっているＯＮＵ（ｎ）が、再度Ｏ８状態に遷移した時に、あらためて初期Ｃｈｕｒｎを実行する。

【０１３３】以上説明したように、ＯＮＵ３０に対して設定更改Ｃｈｕｒｎが失敗した場合には、設定更改失敗フラグを１として、再度初期Ｃｈｕｒｎを行う構成とした。これにより、設定更改Ｃｈｕｒｎの失敗時に、再度初期Ｃｈｕｒｎを行って、Ｃｈｕｒｎｅｄ－ＶＰ設定情報を送信できるので、ＯＬＴ２０とＯＮＵ３０とのＣｈｕｒｎｅｄ－ＶＰ設定情報の設定不一致を防止することが可能になる。

【０１３４】次にフラグ設定制御手段２１の設定更改未完了フラグについて説明する。初期Ｃｈｕｒｎを完了したＯＮＵ３０が、設定更改Ｃｈｕｒｎ失敗以外の何らかの要因で状態落ちした場合には、Ｃｈｕｒｎｅｄ－ＶＰ設定情報の設定更改が終了していないことになる。　そこで、フラグ設定制御手段２１では、設定更改未完了フラグを設け、終了していない場合は、設定更改未完了フラグをセットする。

【０１３５】そして、暗号化設定情報送信制御手段２２は、該当するＯＮＵが再度Ｏ８状態へ遷移した時に、設定更改未完了フラグをチェックし、フラグがセットされていれば初期Ｃｈｕｒｎを実行する。

【０１３６】図１９は設定更改未完了フラグを用いた初期Ｃｈｕｒｎ処理手順を示すフローチャートである。

〔Ｓ９０〕ＯＮＵ（ｎ）が状態落ちした場合は、設定更改が未完了であることを示す設定更改未完了フラグ（ｎ）を１とする。

〔Ｓ９１〕暗号化設定情報送信制御手段２２は、ＯＮＵ（ｎ）に対する各種メッセージの送信を中断する。ＯＮＵ（ｎ）は停止状態となる。

〔Ｓ９２〕暗号化設定情報送信制御手段２２は、設定更改未完了フラグ（ｎ）が１となっているＯＮＵ（ｎ）が、再度Ｏ８状態に遷移した時に、あらためて初期Ｃｈｕｒｎを実行する。

【０１３７】以上説明したように、ＯＮＵ３０の状態落ちが発生した場合には、設定更改未完了フラグを１として、再度初期Ｃｈｕｒｎを行う構成とした。これにより、設定更改Ｃｈｕｒｎ失敗以外の場合でも、再度初期Ｃｈｕｒｎを行って、Ｃｈｕｒｎｅｄ－ＶＰ設定情報を送信できるので、ＯＬＴ２０とＯＮＵ３０とのＣｈｕｒｎｅｄ－ＶＰ設定情報の設定不一致を防止することが可能になる。

【０１３８】次にフラグ設定制御手段２１のＣｈｕｒｎ更改中フラグについて説明する。Ｃｈｕｒｎ更改周期の期間中に、設定更改Ｃｈｕｒｎ等（上書き処理も含め）を行うと、Ｃｈｕｒｎ更改と設定更改Ｃｈｕｒｎが輻輳する可能性があり、設定更改Ｃｈｕｒｎが正常に行われない場合がある。

【０１３９】したがって、フラグ設定制御手段２１は、Ｃｈｕｒｎ更改フラグを設け、Ｃｈｕｒｎ更改周期中はこのフラグをセットする。Ｃｈｕｒｎ更改中フラグがセットしている期間（ＯＬＴ２０から送信されるメッセージの送信禁止期間となる）に、ＯＮＵ３０からＣｈｕｒｎｅｄ－ＶＰ設定情報の更改要求等があった場合は、要

求をｗａｉｔさせ、Ｃｈｕｒｎ更改終了後に設定更改Ｃｈｕｒｎを実行する。これにより、ＯＬＴ２０とＯＮＵ３０とのＣｈｕｒｎｅｄ－ＶＰ設定情報の設定不一致を防止することが可能になる。

【０１４０】次にフラグ設定制御手段２１の設定更改要求フラグについて説明する。初期Ｃｈｕｒｎが完了した運用中のＯＮＵに対し、ＯＬＴ２０が設定更改Ｃｈｕｒｎを行う場合は、外部の保守端末装置よりＯＮＵ単位に設定更改要求フラグをＯＬＴ２０にセットする。

【０１４１】ＯＬＴ２０は、設定更改要求フラグがセットされたＯＮＵに対し、設定更改Ｃｈｕｒｎを行う。設定更改Ｃｈｕｒｎ完了で設定更改要求フラグをクリアする。これにより、初期Ｃｈｕｒｎで設定したＣｈｕｒｎｅｄ－ＶＰ設定情報をＯ８状態中に更改することが可能になる。

【０１４２】一方、設定更改要求フラグは、ＯＮＵ単位とし、１回の設定更改で１ＯＮＵにつき１ＶＰＩの更改に制限する。このため、同報のＶＰＩの設定更改の場合には、すべてのＯＮＵに対し同一設定ができる。

【０１４３】また、１ＯＮＵにつき１ＶＰＩと制限することで、１回の設定更改Ｃｈｕｒｎは、Ｃｈｕｒｎ更改周期内で完了できるため、Ｃｈｕｒｎ設定更改処理時間を明確に規定できる。

【０１４４】次にフラグ設定制御手段２１の設定更改実行中フラグについて説明する。設定更改Ｃｈｕｒｎは、Ｃｈｕｒｎｅｄ－ＶＰ設定情報の設定更改処理であるため処理の優先順位が高い。そこで設定更改実行中フラグを設け、実行中はこのフラグをセットする。

【０１４５】設定更改実行中フラグのセット中は、他のＯＮＵからの要求をｗａｉｔさせることで割り込みを防止し、Ｃｈｕｒｎ設定更改の処理の優先順位を高くする。次に設定更改Ｃｈｕｒｎの処理手順について図２０～図２３を用いて説明する。図２０、図２１は設定更改Ｃｈｕｒｎ開始時の処理手順を示すフローチャートである。

〔Ｓ１００〕暗号化設定情報送信制御手段２２は、設定更改要求フラグが１か否かを判断する（配下のＯＮＵ３０ａ～３０ｎの１ＯＮＵでも設定更改要求があるか否かを判断する）。１ならばステップＳ１０１へ、０ならば終了する。

〔Ｓ１０１〕暗号化設定情報送信制御手段２２は、ＳＥＮＤフラグ（フラグ設定制御手段２１は、ＯＬＴ２０がＣｈｕｒｎｅｄ－ＶＰ設定情報を送信している場合は、ＳＥＮＤフラグをセットする）をチェックする。

【０１４６】ＳＥＮＤフラグが１であれば０になるまで待機し（ステップＳ１０１を繰り返す）、ＳＥＮＤフラグが０ならステップＳ１０２へ行く。

〔Ｓ１０２〕フラグ設定制御手段２１は、ＳＥＮＤフラグをあらためて１にセットして、その他の要求を受け付けないようにする。

【０１４７】ここで、ステップＳ１０３以降から並列処理となる。例えば、ＯＮＵ３０ａ、３０ｂ及び３０ｃに対して設定更改要求があったものとすると、ＯＮＵ３０ａ、３０ｂ及び３０ｃの３つの並列処理が行われる。以降では、ＯＮＵ３０ａに対する設定更改Ｃｈｕｒｎの処理を説明する。

〔Ｓ１０３〕フラグ設定制御手段２１は、設定更改要求フラグを０にする。

〔Ｓ１０４〕フラグ設定制御手段２１は、設定更改実行中フラグを１にする。

〔Ｓ１０５〕暗号化設定情報送信制御手段２２は、Ｃｈｕｒｎｅｄ－ＶＰ設定情報に更改ＶＰＩをセットし、Ｃｈｕｒｎｅｄ－ＶＰ設定情報の送信回数ｋ（例えば、ｋ＝３）を設定する。

〔Ｓ１０６〕暗号化設定情報送信制御手段２２は、Ｃｈｕｒｎ更改中フラグが１か否かを判断する。１の場合は０になるまで待機し（ステップＳ１０６を繰り返す）、０の場合はステップＳ１０７へ行く。

〔Ｓ１０７〕ＯＮＵ３０ａがＯ８状態から状態落ちしたか否かを判断する。すなわち、設定更改未完了フラグをチェックし、フラグが１ならばステップＳ１１０へ行き、フラグが０ならステップＳ１０８へ行く。

〔Ｓ１０８〕暗号化設定情報送信制御手段２２は、Ｃｈｕｒｎｅｄ－ＶＰ設定情報を送信し、Ｃｈｕｒｎｅｄ－ＶＰ設定情報を１回送信する度にｋから１をデクリメント（ｋ＝ｋ－１）し、送信回数を管理する。

〔Ｓ１０９〕ｋ＝０なら終了し、ｋ≠０ならステップＳ１０６へ戻る。

〔Ｓ１１０〕暗号化設定情報送信制御手段２２は、初期Ｃｈｕｒｎを行う。

【０１４８】図２２はＡＣＫメッセージの受信処理時のフローチャートを示す図である。ＯＬＴ２０がＣｈｕｒｎｅｄ－ＶＰ設定情報を送信した場合、ＯＮＵ３０ａが正常にＣｈｕｒｎｅｄ－ＶＰ設定情報を受信すると、ＡＣＫメッセージをＯＬＴ２０へ返送する。

〔Ｓ１２０〕暗号化設定情報送信制御手段２２からＣｈｕｒｎｅｄ－ＶＰ設定情報の送信後（例えば、３回送信した後）、一定時間内（例えば、３００ｍｓ以内）でＡＣＫメッセージの返答があるか計測する。タイムアウトした場合はステップＳ１２３へ、そうでなければステップＳ１２１へ行く。

〔Ｓ１２１〕Ｃｈｕｒｎ更改中フラグが１か否かを判断する。１の場合は０になるまで待機し（ステップＳ１２１を繰り返す）、０の場合はステップＳ１２２へ行く。

〔Ｓ１２２〕フラグ設定制御手段２１は、設定更改実行中フラグを０にする。

〔Ｓ１２３〕フラグ設定制御手段２１は、設定更改失敗フラグを１にする。

〔Ｓ１２４〕暗号化設定情報送信制御手段２２は、初期Ｃｈｕｒｎを行う。

【０１４９】図２３は設定更改Ｃｈｕｒｎ終了時のフローチャートを示す図である。

〔Ｓ１３０〕すべてのＯＮＵの設定更改実行中フラグを監視し、設定更改実行中フラグがすべて０ならば、処理完了となりステップＳ１３１へ行く。そうでなければ０になるまで設定更改実行中フラグを監視し続ける（ステップＳ１３０を繰り返す）。

〔Ｓ１３１〕ＳＥＮＤフラグを０にして、他の処理に解放する。

【０１５０】次に暗号化設定情報上書き手段２３について説明する。初期Ｃｈｕｒｎ完了後、Ｃｈｕｒｎｅｄ－ＶＰ設定情報の設定更改がなければ、その後、ＯＬＴ２０がＯＮＵ３０に対してＣｈｕｒｎｅｄ－ＶＰ設定情報を送信することはない。

【０１５１】このため、従来では何らかの原因で、ＯＬＴ２０とＯＮＵ３０とのＣｈｕｒｎｅｄ－ＶＰ設定情報が設定不一致となった場合でも不一致となった状態を確認することができなかった。

【０１５２】そこで、本発明では暗号化設定情報上書き手段２３を設け、ＯＮＵ３０が運用中、初期Ｃｈｕｒｎ完了をトリガとして、Ｃｈｕｒｎｅｄ－ＶＰ設定情報の上書き処理である上書きＣｈｕｒｎを実行させることにした。これにより、何らかの原因でＯＬＴ２０とＯＮＵ３０とのＣｈｕｒｎｅｄ－ＶＰ設定情報が設定不一致となった場合でも、上書きＣｈｕｒｎで一致させることができる。

【０１５３】また、上書きＣｈｕｒｎは、ＯＬＴ２０とＯＮＵ３０とのＣｈｕｒｎｅｄ－ＶＰ設定情報を一致させるための保護機能であるため、処理の優先順位は低くて構わない。

【０１５４】そこで、上書きＣｈｕｒｎのＣｈｕｒｎｅｄ－ＶＰ設定情報に対する送信要求は、他のメッセージ送信要求がある場合や設定更改Ｃｈｕｒｎを行っている等の場合はｗａｉｔさせて、上書きＣｈｕｒｎの優先順位を低くする。これにより、他のメッセージ送信を圧迫せずに、上書きＣｈｕｒｎを実行できる。

【０１５５】さらに、暗号化設定情報上書き手段２３の内部には、上書きＣｈｕｒｎを実行するためのタイマが設けられる。このタイマは、上書きＣｈｕｒｎ用のＣｈｕｒｎｅｄ－ＶＰ設定情報の送信後に起動し、上書きＣｈｕｒｎを行うべき最低限の周期を計測する。

【０１５６】そして、タイマで計測された次の送信時刻（他のメッセージ送信と競合しないように設定される）がくるまでは、上書きＣｈｕｒｎ用のＣｈｕｒｎｅｄ－ＶＰ設定情報は送信しない。

【０１５７】また、タイマの設定周期は、保守端末装置を通じて、任意の値を設定できる。したがって、上書きＣｈｕｒｎ設定に柔軟性を持たせることができる。次にＣｈｕｒｎｉｎｇ－Ｋｅｙアップデートメッセージと、Ｃｈｕｒｎｅｄ－ＶＰ設定情報との送信時の競合防止について説明する。

【０１５８】ＩＴＵ－Ｔ勧告Ｇ．９８３では、ＯＮＵ３０へのメッセージは、一定周期に発生する下りＰＬＯＡＭセルにより送信される。したがって、ＰＬＯＡＭセル周期で送信すべきメッセージの調停処理を行って、ＯＮＵ３０へ送信するメッセージを決定しなければならない。

【０１５９】Ｃｈｕｒｎｉｎｇ－Ｋｅｙアップデートメッセージは、図５で上述したように１６×Ｔフレーム間隔で送信される。また、Ｃｈｕｒｎｅｄ－ＶＰ設定情報は、Ｃｈｕｒｎ更改中フラグがセットされていない間で、３回の送信を完了する必要がある。

【０１６０】暗号化設定情報送信制御手段２２は、Ｃｈｕｒｎｉｎｇ－Ｋｅｙアップデートメッセージと、Ｃｈｕｒｎｅｄ－ＶＰ設定情報との調停処理を行った場合には、Ｃｈｕｒｎｉｎｇ－Ｋｅｙアップデートメッセージを優先する。

【０１６１】すると、Ｃｈｕｒｎｉｎｇ－Ｋｅｙアップデートメッセージは、１６×Ｔフレーム間隔に自動的に送信される。その後、Ｃｈｕｒｎｅｄ－ＶＰ設定情報が例えば１６×Ｔフレーム間隔で３回自動的に送信される。

【０１６２】すなわち、Ｃｈｕｒｎｉｎｇ－Ｋｅｙアップデートメッセージと、Ｃｈｕｒｎｅｄ－ＶＰ設定情報の初回のみが調停対象となり、初回のＣｈｕｒｎｉｎｇ－Ｋｅｙアップデートメッセージが送信されれば２回目、３回目のメッセージ送信は互いに競合を起こすことなく自動的に送信することが可能になる。

【０１６３】次に暗号化設定情報更改手段２４について説明する。ＩＴＵ－Ｔ勧告Ｇ．９８３では、Ｃｈｕｒｎｉｎｇ－Ｋｅｙ更改タイミングは規定されているが、Ｃｈｕｒｎｅｄ－ＶＰ設定情報の更改タイミングは規定されていない。このため、ＯＬＴ２０ではＣｈｕｒｎｅｄ－ＶＰ設定情報に対して、不規則に設定情報の更改を行うと、ＯＬＴ２０とＯＮＵ３０とのＣｈｕｒｎｅｄ－ＶＰ設定情報の設定不一致を起こしてしまう可能性がある。

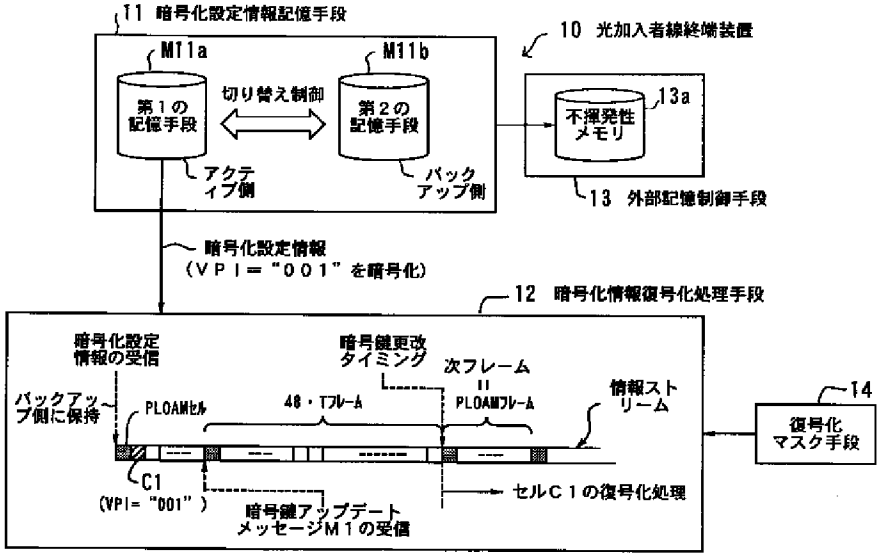
【０１６４】そこで、暗号化設定情報更改手段２４は、Ｃｈｕｒｎｉｎｇ－Ｋｅｙ更改タイミングでＣｈｕｒｎｅｄ－ＶＰ設定情報の更改を行うことにして不一致を防止する。

【０１６５】図２４はＣｈｕｒｎｅｄ－ＶＰ設定情報の更改を示す図である。Ｃｈｕｒｎｅｄ－ＶＰ設定情報を３回送信完了後の最初のＣｈｕｒｎｉｎｇ－Ｋｅｙ更改タイミングｔで、送信されたＣｈｕｒｎｅｄ－ＶＰ設定情報に対する設定更改を行っていく。

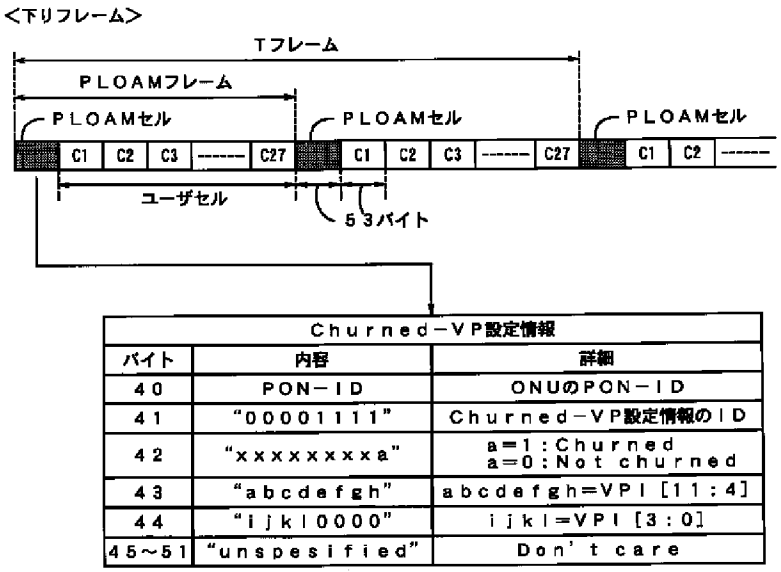
【０１６６】これにより、ＯＬＴ２０とＯＮＵ３０間でＣｈｕｒｎｅｄ－ＶＰ設定情報の設定更改を同期して行うことが可能になり、Ｃｈｕｒｎｅｄ－ＶＰ設定情報の設定不一致を防止することが可能になる。

【０１６７】
【発明の効果】以上説明したように、本発明の光加入者線終端装置は、現在使用中の暗号化設定情報を記憶するアクティブ側の第１の記憶手段と、新しく更改された暗号化設定情報を記憶するバックアップ側の第２の記憶手段との切り替え制御を行い、読み出した暗号化設定情報にもとづいて、次フレームの先頭から暗号化された情報部分の復号化処理を行う構成とした。これにより、暗号化設定情報の送信側と受信側との暗号化・復号化の処理タイミングのずれを防止し、高品質な通信制御を行うことが可能になる。
【０１６８】また、本発明の光加入者線端局装置は、受信装置へ情報ストリームを送信する際に、フラグの設定制御を行い、フラグにもとづいて、暗号化設定情報の送信制御を行う構成とした。これにより、暗号化設定情報の送信側と受信側との暗号化・復号化の処理タイミングのずれを防止し、高品質な通信制御を行うことが可能になる。
【図面の簡単な説明】
【図１】本発明の光加入者線終端装置の原理図である。
【図２】情報ストリームの構成及びＣｈｕｒｎｅｄ－ＶＰ設定情報のフォーマットを示す図である。
【図３】Ｃｈｕｒｎｉｎｇ－Ｋｅｙの更改シーケンスを示す図である。
【図４】２面ＲＡＭを持つＯＮＵのブロック構成を示す図である。
【図５】コピー動作手順を示すフローである。
【図６】コピー動作時のタイミングチャートを示す図である。
【図７】コピー中にＣｈｕｒｎｅｄ－ＶＰ設定情報を受信した際の動作を示すタイミングチャートである。
【図８】応答信号の返送制御手順を示すフローチャートである。
【図９】更改されたＣｈｕｒｎｅｄ－ＶＰ設定情報をＳＲＡＭから不揮発性メモリへ記憶させる場合の処理手順を示すフローチャートである。
【図１０】暗号化設定情報記憶手段の電源復旧時の動作状態を示すフローチャートである。
【図１１】復号化マスク処理を示す図である。
【図１２】ＯＮＵの変形例を示す図である。
【図１３】次フレームでＤｅｃｈｕｒｎを実現するためのブロック構成を示す図である。
【図１４】次フレームからＤｅｃｈｕｒｎを行う際のタイミングチャートを示す図である。
【図１５】本発明の光加入者線端局装置の原理図である。
【図１６】初期Ｃｈｕｒｎフラグを用いた初期Ｃｈｕｒｎ処理手順を示すフローチャートである。
【図１７】初期Ｃｈｕｒｎ実行中フラグを用いた初期Ｃｈｕｒｎ処理手順を示すフローチャートである。
【図１８】設定更改失敗フラグを用いた初期Ｃｈｕｒｎ処理手順を示すフローチャートである。
【図１９】設定更改未完了フラグを用いた初期Ｃｈｕｒｎ処理手順を示すフローチャートである。
【図２０】設定更改Ｃｈｕｒｎ開始時の処理手順を示すフローチャートである。
【図２１】設定更改Ｃｈｕｒｎ開始時の処理手順を示すフローチャートである。
【図２２】ＡＣＫメッセージの受信処理時のフローチャートを示す図である。
【図２３】設定更改Ｃｈｕｒｎ終了時のフローチャートを示す図である。
【図２４】Ｃｈｕｒｎｅｄ－ＶＰ設定情報の更改を示す図である。
【図２５】ＡＴＭ－ＰＯＮシステムの構成を示す図である。
【符号の説明】
１０　光加入者線終端装置
１１　暗号化設定情報記憶手段
１２　暗号化設定情報復号化処理手段
１３　外部記憶制御手段
１３ａ　不揮発性メモリ
１４　復号化マスク手段
Ｍ１１ａ　第１の記憶手段
Ｍ１１ｂ　第２の記憶手段
【手続補正２】
【補正対象書類名】図面
【補正対象項目名】全図
【補正方法】変更
【補正内容】

【図１】

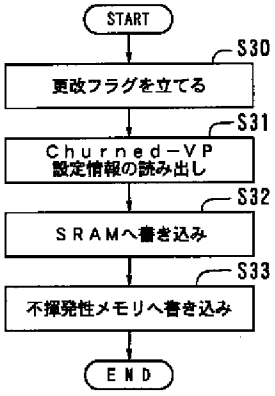


【図２】

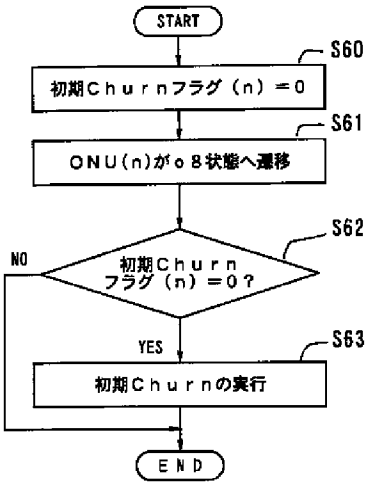


Ｃｈｕｒｎｅｄ－ＶＰ設定情報		
バイト	内容	詳細
４０	ＰＯＮ－ＩＤ	ＯＮＵのＰＯＮ－ＩＤ
４１	"００００１１１１"	Ｃｈｕｒｎｅｄ－ＶＰ設定情報のＩＤ
４２	"ｘｘｘｘｘｘｘｘａ"	ａ＝１：Ｃｈｕｒｎｅｄ ａ＝０：Ｎｏｔ ｃｈｕｒｎｅｄ
４３	"ａｂｃｄｅｆｇｈ"	ａｂｃｄｅｆｇｈ＝ＶＰＩ［１１：４］
４４	"ｉｊｋｌ０００"	ｉｊｋｌ＝ＶＰＩ［３：０］
４５～５１	"ｕｎｓｐｅｓｉｆｉｅｄ"	Ｄｏｎ'ｔ ｃａｒｅ

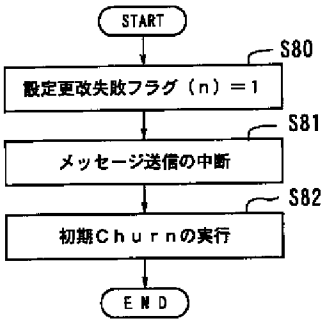
【図９】



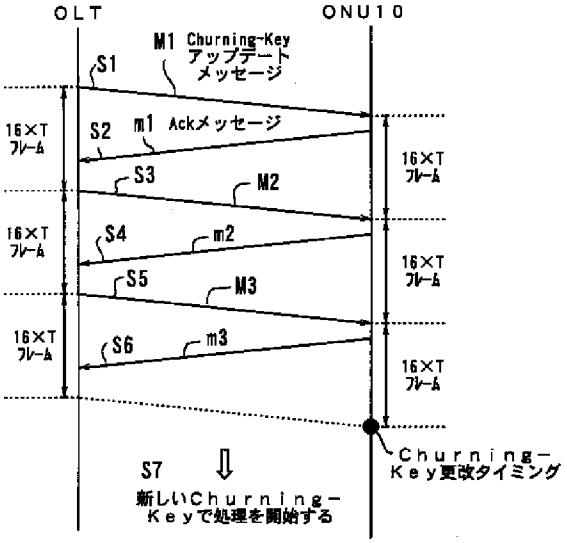
【図１６】



【図１８】

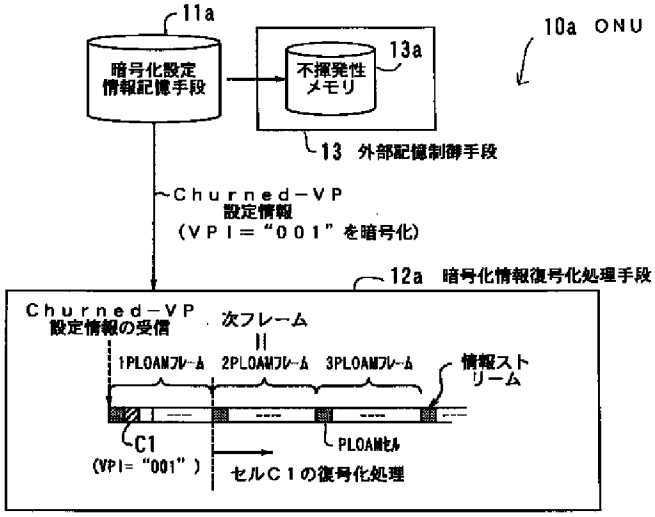


【図３】

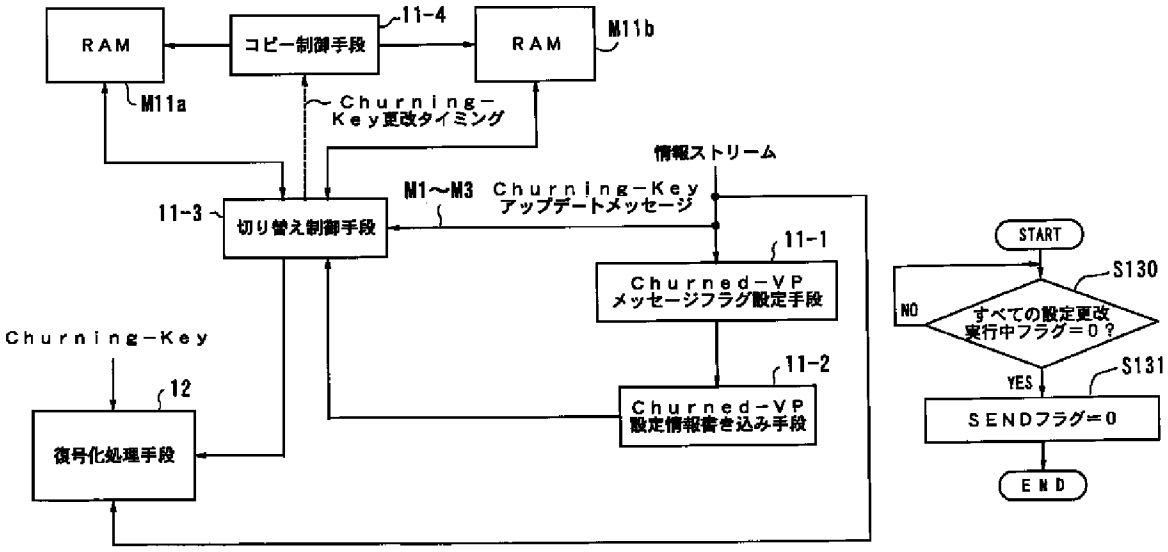


【図４】

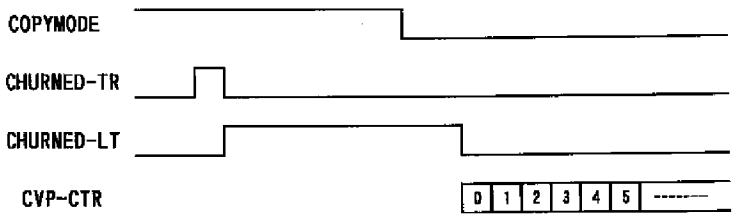
【図１２】



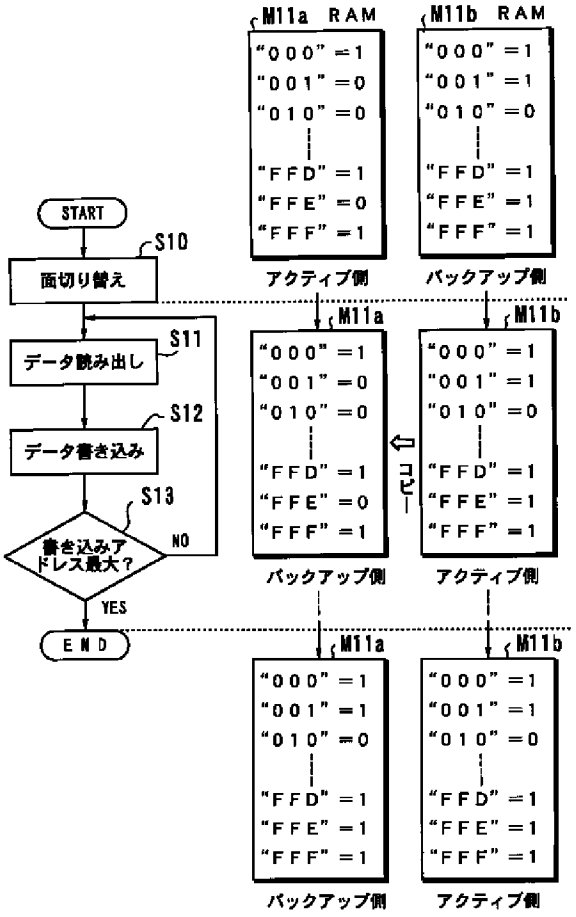
【図２３】



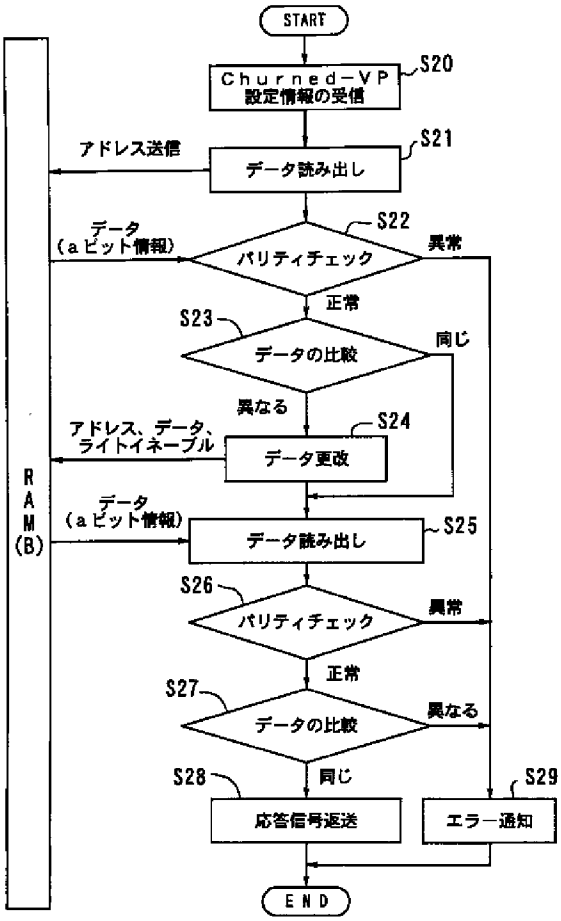
【図７】



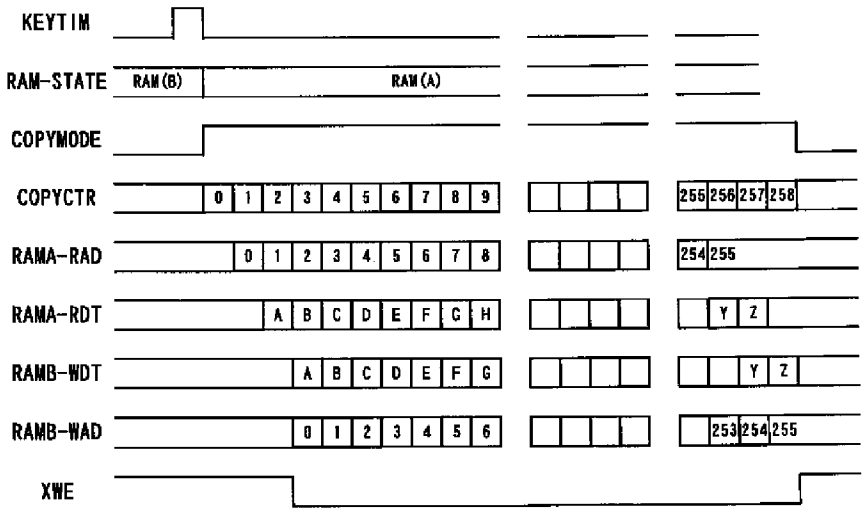
【図５】


M11a RAM
M11b RAM
"000"=1
"001"=0
"010"=0
"FFD"=1
"FFE"=0
"FFF"=1
START
S10
面切り替え
S11
データ読み出し
S12
データ書き込み
S13
書き込みアドレス最大？
NO
YES
END
アクティブ側
バックアップ側
コピー

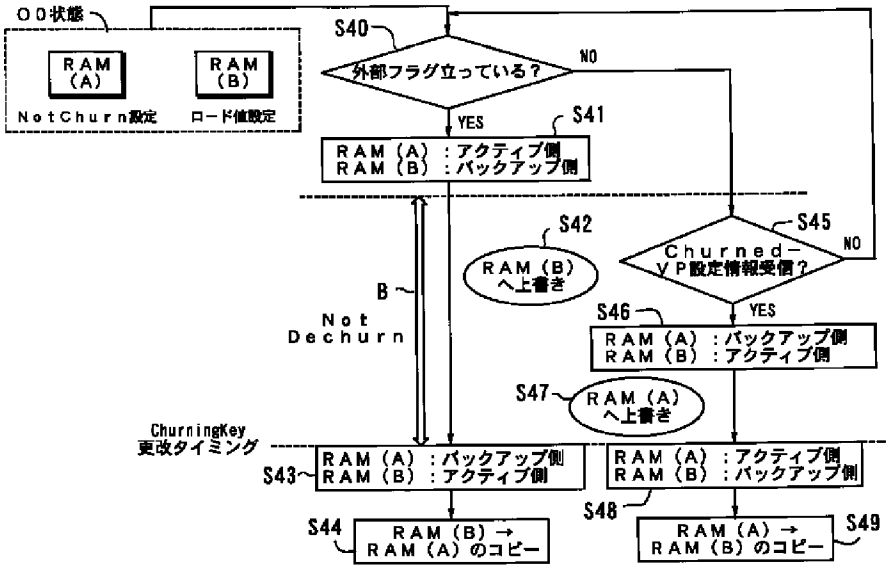
【図８】


START
S20
Churned-VP 設定情報の受信
S21
データ読み出し
アドレス送信
S22
データ (aビット情報)
パリティチェック
異常
正常
S23
データの比較
同じ
異なる
S24
アドレス、データ、ライトイネーブル
データ更改
RAM (B)
データ (aビット情報)
S25
データ読み出し
S26
パリティチェック
異常
正常
S27
データの比較
異なる
同じ
S28
応答信号返送
S29
エラー通知
END

【図６】

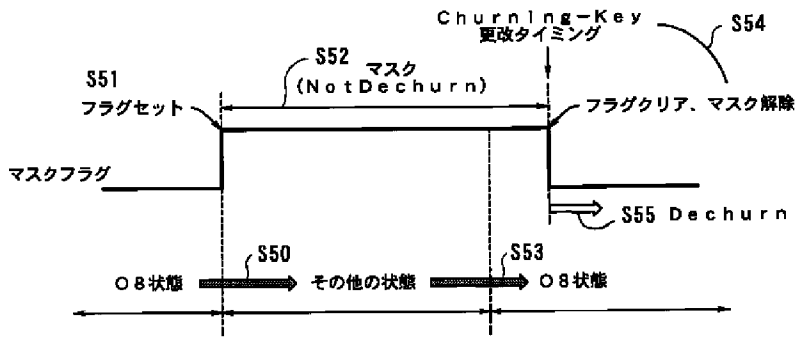

KEYTIM
RAM-STATE
RAM(B)
RAM(A)
COPYMODE
COPYCTR
RAMA-RAD
RAMA-RDT
RAMB-WDT
RAMB-WAD
XWE

【図１０】

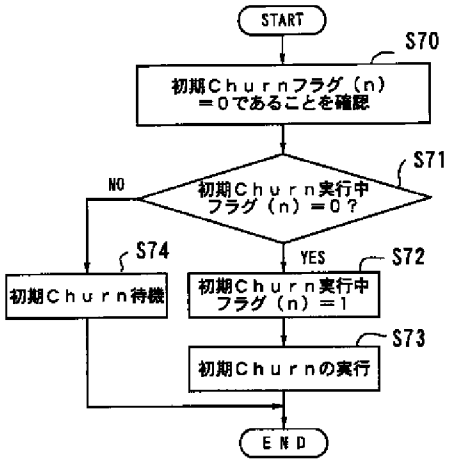


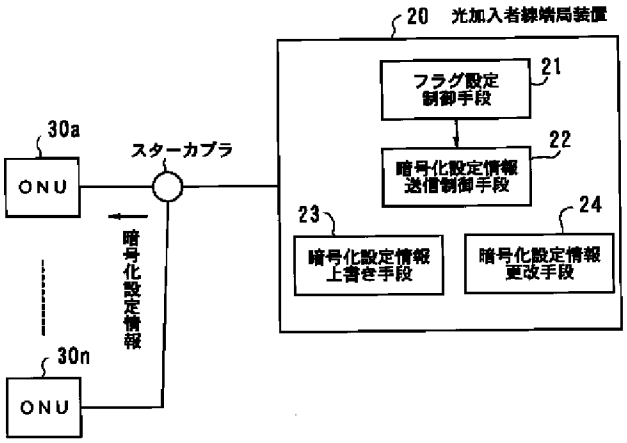
【図１１】

【図１７】

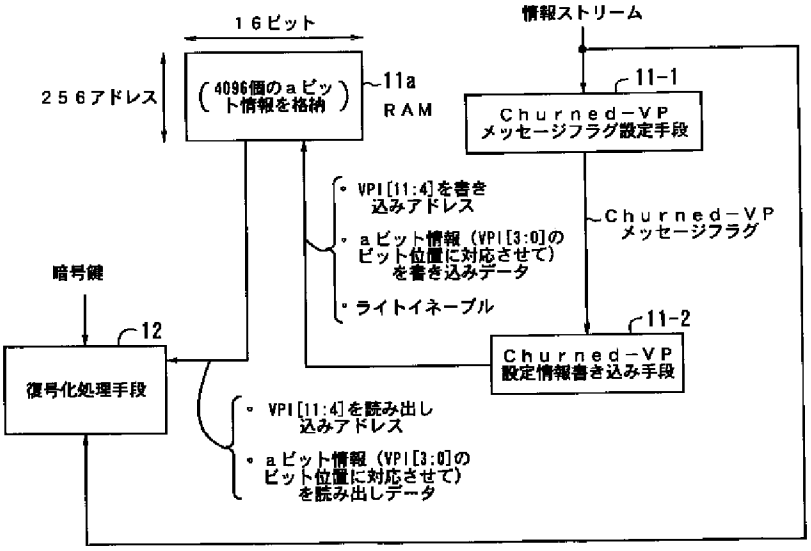


【図１５】

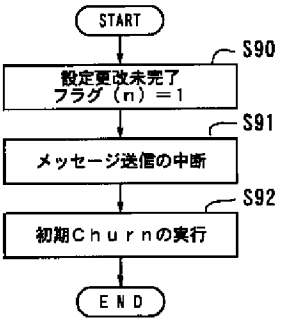




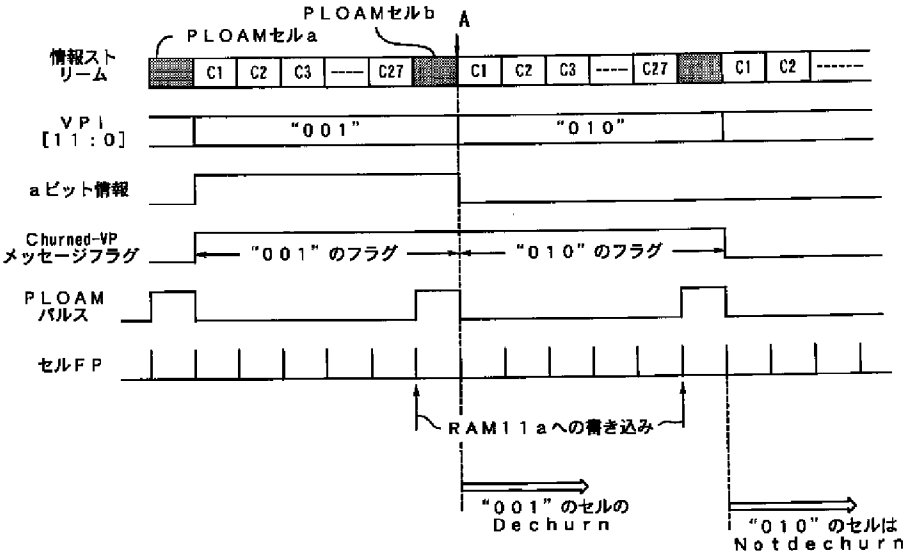
【図１３】


１６ビット
２５６アドレス
（4096個のａビット情報を格納）
11a
RAM
情報ストリーム
11-1
Ｃｈｕｒｎｅｄ－ＶＰ
メッセージフラグ設定手段
Ｃｈｕｒｎｅｄ－ＶＰ
メッセージフラグ
・VPI[11:4]を書き込みアドレス
・ａビット情報（VPI[3:0]のビット位置に対応させて）を書き込みデータ
・ライトイネーブル
暗号鍵
12
復号化処理手段
11-2
Ｃｈｕｒｎｅｄ－ＶＰ
設定情報書き込み手段
・VPI[11:4]を読み出し込みアドレス
・ａビット情報（VPI[3:0]のビット位置に対応させて）を読み出しデータ

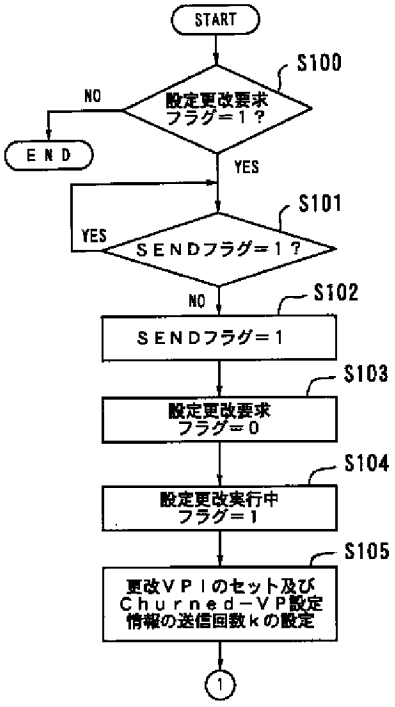
【図１９】


START
S90
設定更改未完了
フラグ（ｎ）＝1
S91
メッセージ送信の中断
S92
初期Ｃｈｕｒｎの実行
ＥＮＤ

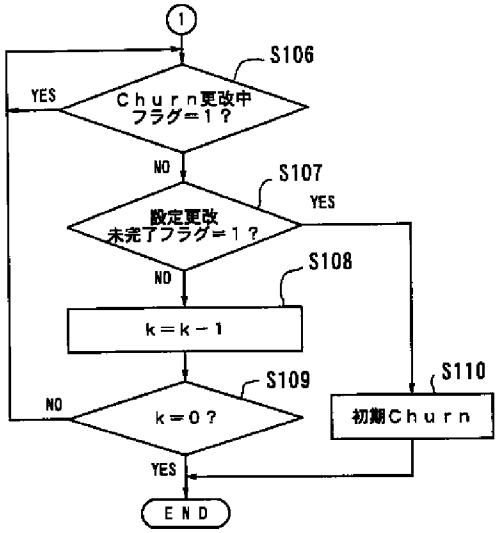
【図１４】


PLOAMセルb
A
PLOAMセルa
情報ストリーム
C1
C2
C3
C27
VPI[11:0]
"001"
"010"
aビット情報
Churned-VP
メッセージフラグ
"001"のフラグ
"010"のフラグ
PLOAM
パルス
セルFP
RAM11aへの書き込み
"001"のセルの
Dechurn
"010"のセルは
Notdechurn

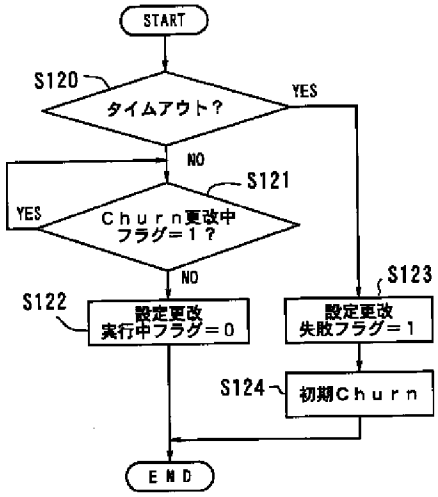
【図２０】


START
S100
設定更改要求
フラグ＝１？
NO
ＥＮＤ
YES
S101
YES
ＳＥＮＤフラグ＝１？
NO
S102
ＳＥＮＤフラグ＝１
S103
設定更改要求
フラグ＝０
S104
設定更改実行中
フラグ＝１
S105
更改ＶＰＩのセット及び
Ｃｈｕｒｎｅｄ－ＶＰ設定
情報の送信回数ｋの設定
①

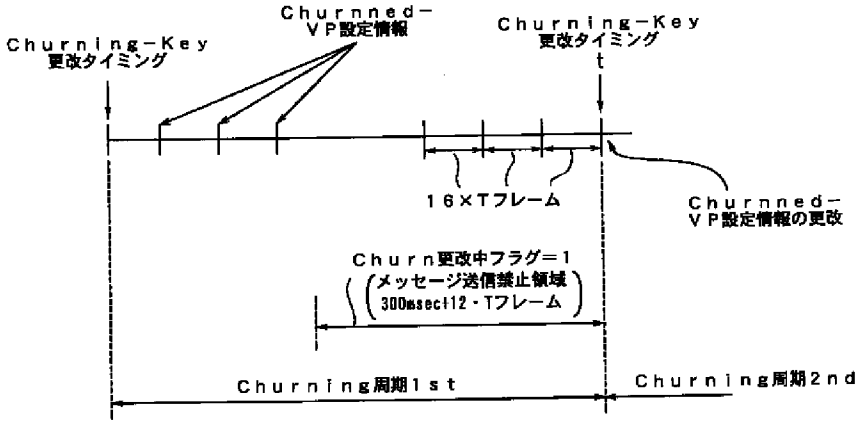
【図２１】


①
S106
YES
Ｃｈｕｒｎ更改中
フラグ＝１？
NO
S107
YES
設定更改
未完了フラグ＝１？
NO
S108
ｋ＝ｋ－１
S109
NO
ｋ＝０？
YES
S110
初期Ｃｈｕｒｎ
ＥＮＤ

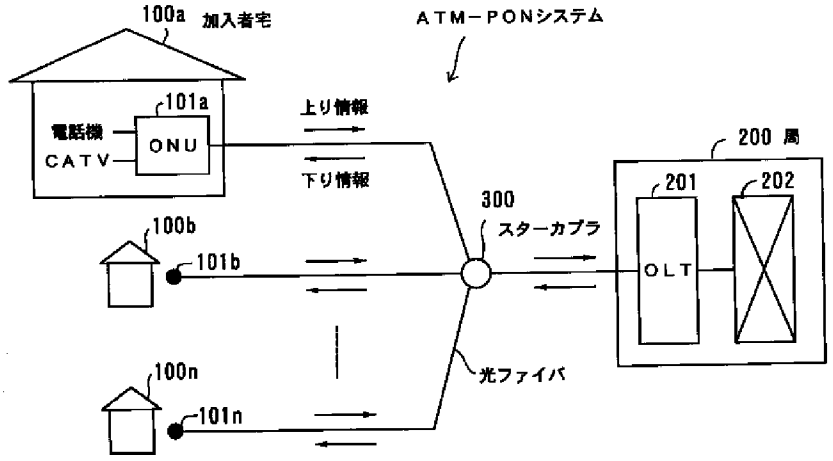
【図２２】


START
S120
タイムアウト？
YES
NO
S121
YES
Ｃｈｕｒｎ更改中
フラグ＝１？
NO
S123
S122
設定更改
実行中フラグ＝０
設定更改
失敗フラグ＝１
S124
初期Ｃｈｕｒｎ
ＥＮＤ

【図２４】



【図２５】



フロントページの続き

(51)Int.Cl.[7]	識別記号	F I	ﾃｰﾏｺｰﾄﾞ(参考)
H04Q 11/04		H04Q 11/04	B 9A001

(72)発明者 三浦 健司
大阪府大阪市中央区城見２丁目２番６号
富士通関西ディジタル・テクノロジ株式会社内
(72)発明者 松尾 保
大阪府大阪市中央区城見２丁目２番６号
富士通関西ディジタル・テクノロジ株式会社内
(72)発明者 塩野 秀樹
大阪府大阪市中央区城見２丁目２番６号
富士通関西ディジタル・テクノロジ株式会社内
(72)発明者 豊田 好美
大阪府大阪市中央区城見２丁目２番６号
富士通関西ディジタル・テクノロジ株式会社内

(72)発明者　小柳　敏則
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
(72)発明者　阿比留　節雄
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
(72)発明者　安里　淳
大阪府大阪市中央区城見２丁目２番６号　富士通関西ディジタル・テクノロジ株式会社内
(72)発明者　藤吉　新一
福岡県福岡市博多区博多駅前三丁目22番８号　富士通九州ディジタル・テクノロジ株式会社内
(72)発明者　内田　和宏
福岡県福岡市博多区博多駅前三丁目22番８号　富士通九州ディジタル・テクノロジ株式会社内
(72)発明者　龍　一也
福岡県福岡市博多区博多駅前三丁目22番８号　富士通九州ディジタル・テクノロジ株式会社内
(72)発明者　平島　勝彦
福岡県福岡市博多区博多駅前三丁目22番８号　富士通九州ディジタル・テクノロジ株式会社内
(72)発明者　四丸　建夫
福岡県福岡市博多区博多駅前三丁目22番８号　富士通九州ディジタル・テクノロジ株式会社内
(72)発明者　若吉　光春
福岡県福岡市博多区博多駅前三丁目22番８号　富士通九州ディジタル・テクノロジ株式会社内
(72)発明者　酒井　俊行
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

Ｆターム(参考)　5J104 AA01 AA16 AA34 NA02 NA37 PA00 PA06
5K002 AA03 AA04 DA05 DA12 EA03 FA01
5K030 GA11 GA15 HA10 HB14 JA08 JL03 JL08 KA04 KA13 KA21 LA07 LA12 LE05 MC07 MD02
5K033 AA05 AA07 AA08 CB15 CB17 DA15 DB10 DB12 DB22 EB06
5K069 AA10 BA10 CA02 CB01 CB05 DA06 EA11 EA24 FC06 HA09
9A001 BB02 BB03 BB04 CC04 CC07 DD08 DD10 EE03 JJ18 JJ20 KK16 KK43 KK56 LL02 LL03 LL05